A seat at the table

The shifting paradigm for Government IT infrastructure

A scaled, secure and sovereign future with research insights

Publicsectornetwork.co (02) 9057 9070

PUBLIC SECTOR NETWORK

Contents

Executive Summary

NSW has been one of Australia's leaders in the transformation of citizen experiences with agencies like Service NSW, Police and the Department of Transport adopting cutting edge capabilities to power the delivery of their services - many of which have won awards and acclaim. Much of this has been enabled by the IT departments using the NSW Government Data Centre (GovDC) and embracing public cloud computing. This is the infrastructure that allows services to be delivered.

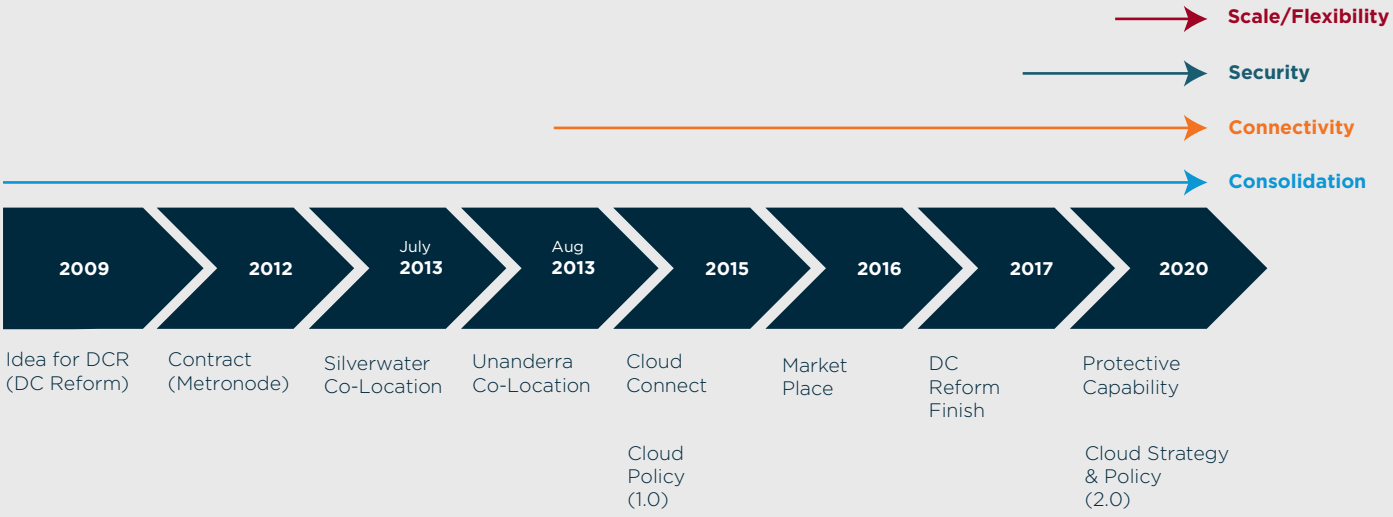
It is not possible to understand the future of IT infrastructure in NSW Government without understanding

- The profound effect that GovDC has played and will continue to play in the transformation and digital journey of NSW Government.
- That agencies will seek to locate compute and storage close to where it is consumed. The practice of bringing data, compute and capability close to where it is consumed is known as "Edge" or Edge Computing.
- The rise of IoT and the explosion of data will also mean that it will become increasingly difficult to manage performance and centralise all data.
- IT finally has a seat at the table rather than being relegated to the back end of Government
- Trends around public, private, distributed cloud delivering fit for purpose configurations. Flexibility and security are in the forefront of everyone's minds.
- COVID-19 - has changed things significantly
- Security and the geo-political consequences will have agencies reconsidering their assets and posture
- Cyber and data security sensitivities are elevated. State-based actors have changed the landscape irrevocably.
- WFA (Work from Anywhere) will replace WFO (Work from Office) and WFH (Work from Home).

This report intends to inform and spark discussion on the new patterns for IT infrastructure, storage and compute and will be useful for IT leaders within state and local Governments who are seeking to leverage Government-owned Data Centres, edge and public cloud for better outcomes.

While it borrows heavily from examples and interviews in NSW, the findings and learnings can be applied across Government in Australia.

Background: GovDC - a remarkable contribution to NSW



A little GovDC history

GovDC had its genesis in the DCR (Data Centre Reform) program when it became apparent that the multitude of agency owned and run Data Centres were inefficient and risky. This resulted in two consolidated Government Data Centres - Silverwater (Sydney) and Unanderra (Wollongong). A mandate directed agencies to migrate off their existing Data Centres and precluded other Data Centre co-location. GovDC utilisation is now significant but each agency has its own DR and business continuity strategy.

Cloud connect was made available in 2015 allowing GovDC infrastructure to easily connect to the public cloud. This was followed by GovDC marketplace (for vendors to create and deliver GovDC specific products).

These services helped consolidate the number of firewalls and internet connections across NSW Government - narrowing the attack surface and concentrating expertise, capability and services. This has paved the way for agencies to easily connect their infrastructure to the public cloud and enabled public cloud adoption.

GovDC success is evidenced by the consolidation of more than 130 Data Centres under the program into two secure and efficient centralised locations and connected this to the cloud.

Recent Changes

The just-released Cloud Strategy and Cloud policy recently provides Public cloud first guidance and aligns older policies. Importantly it creates crucial shifts in security and allows GovDC to truly transcend the geographic constraints of Silverwater and Unanderra. GovDC can now exist in secure physical locations and closer to customers with elevated security needs.

The NSW Government Cloud Strategy sets the vision, principles, and outcomes for cloud use across the NSW Government, as well as the roadmap for overcoming existing challenges.

The NSW Government Cloud Policy guides and direct agency cloud use, in line with existing procurement and security guidance. The Cloud Policy will mandate that NSW agencies use Public cloud services by default and use Government Data Centres (GovDC) for workloads that require

SECURE Higher Physical Security controls and host and operate protected workloads (Zone 3 PSPF Panel)

PRIVATE Cloud (computing resources used exclusively by a single organisation, with services and infrastructure maintained on a private network)

COMMUNITY Cloud - A marketplace and secure environment for the provision of as-a-service solutions from vendors and dedicated to NSW Government agencies

The new strategy and policy also takes into account historic iterations of various digital and cloud strategies and policies, including the NSW Digital Strategy, 'Beyond Digital Strategy', Federal Secure Cloud Strategy, and the Federal Digital Transformation Strategy

Despite infrastructural foundations having a historically low profile, it will become a critical enabler for future applications and digital workloads where workloads are matched to the infrastructure that's required instead of a one size fits all approach.

In essence, GovDC becomes the Private, Secure and Edge Cloud for Government and Public Cloud is first for all other workloads.

Part 1: Scale, Security, Sovereignty

Data will overwhelm

The foundational issue that is going to need solving is data volume and security. The applications of the future will heavily depend on the infrastructure that supports and enables this foundational need. For years IT departments have stored, secured, connected, transmitted, processed and backed up data over their networks. Public cloud helped free up teams with on-demand capacity and programmable infrastructure.

But today's patterns are all about to change. The volume of data that will be coming is a tsunami. Dialling up the storage in GovDC or in a public cloud provider is important but will not solve all problems - because future workloads will be different.

Why this is different

- Globally the 30 billion connected digital devices will grow to 75 billion by 2025. Australia is estimated to be 1% of these devices and is likely to increase this because of our unique geography
- Data is doubling every two years, including Government data - so from here on out the problem will compound each year.
- According to Gartner, connected IoT devices will globally generate 79.4ZB of Data in 2025.
- 5G will enable a whole new generation of connected devices.
- Video on track to become 80% of mobile data traffic by 2022/3. 5G and hi-def will supercharge this after 2022.
- According to IDC, IoT will comprise 20 percent of all data created by 2025.
- Within 8 years, the average person will interact with a connected device nearly 4,800 times a day
- The internet will fundamentally change when Human to Machine volume will be significantly replaced by Machine to Machine.
- Machines will generate and consume most of the data on the internet and probably private and government networks too.

Scaling

There is a profound change to the size and quantity of data will require new models to scale, store and process data. Anticipating and preparing for these changes will be key.

Networks

Infrastructure teams should anticipate that, in the fullness of time, networks will no longer have enough bandwidth to centralise all data. The one size fits all model may no longer work. Workloads will need to be adapted and matched to specific patterns and many types of data will need to be captured, stored, secured and processed at the edge (closer to customers) or in optimised locations. Virtual Reality will increasingly be used in a COVID-19 and a carbon-conscious world to reduce travel - this pattern is intolerant to delays (latency) and anything outside metropolitan use will likely need storage at the edge.

Autonomous vehicles and drones will access and capture vast amounts of data as they travel and will be heavily used in future Spatial, Education, Transport, Mining, Research and Agriculture applications.

5G & IoT

5G is next generation wireless network technology that's expected to change the way people live and work. It will be faster and able to handle more connected devices than the existing 4G network - an improvement that will enable a wave of new kinds of tech products. It will set a new level of expectation for citizens and employees and a new generation of applications will emerge using this technology - healthcare, AI and autonomous functionality. Millions of devices will be connected to networks and the Government will invest heavily in IoT (Internet of Things) and sensors will emerge generating massive amounts of data. While it is easy to focus on the increased speed of 5G (expect 10x faster than 4G) there are also improvements in latency (delays) and the number of devices that can connect to a single tower. The main drawback is that more towers will also be required as the signals will not travel as far.

Regional

Many regional locations suffer from poor connectivity with limited options. Government MPLS networks are expensive to operate for backhaul connectivity back to GovDC. SDN (Software Defined Networks) can significantly reduce these costs when replaced or augmented by NBN connections. Most agencies have large regional footprints due in part to ⅓ of Australians living, working and raising families outside our capital cities. Over 60% of Australia's exports are derived from regional, rural and remote areas including Mining, Farming and Manufacturing - as a result, this will continue to drive Government importance and focus.

AI

AI will increasingly operate at the edge to allow mission-critical and time sensitive decisions to be made faster, more reliably and with greater security. This is being fuelled by the rapid growth of smart devices at the edge. While AI has traditionally been deployed in the cloud (because AI algorithms crunch massive amounts of data and consume massive computing resources) decisions will increasingly need to be made locally, on devices that are close to the edge of the network. As a result, the cloud will move to the edge - either as a private or public cloud. To support this NSW has released its official AI policy.

Capex, Opex and Bill Shock

Traditionally IT relied heavily on Capex investments. While there has been some move to Opex there are many assets that still have a useful life and some agencies still rely on Capex as part of broader projects. When migrating infrastructure to the public cloud it is important that the processes that manage consumption also change. If this is not done, then it is highly likely that agencies will experience bill shock and cloud compute will cost more than expected. Aligning individual workloads to the optimal pattern for compute and storage is key. PUBLIC Cloud for everything is not necessarily correct and predictability will still have an attraction for many agencies and workloads.

NBN

The recently announced fibre investments from the NBN will be a game changer. This provides a real alternative to existing networks at a lower cost and can underpin hybrid PUBLIC/PRIVATE cloud solutions. It can also be used to power Software Defined Networks (SDN) and optimise network performance.

Edge, hybrid and distributed cloud patterns

IT infrastructure currently relies heavily on traditional private Government networks that transport all data to GovDC or cloud for storage and compute. SDN (Software Defined Networks) help offload some of the internet capacity but the explosion in data will mean that it is no longer possible to shift all data to central locations. Data will become distributed because of performance, security, cost and bandwidth.

This will drive the need to embrace the edge - where data will be processed, categorised and stored closest to where it will be consumed. Content will be pushed closer to customers and citizens especially for applications that use real time AI, Artificial Reality or Virtual Reality as these are sensitive to latency.

Forbes predicts in its Top 10 Digital Transformation Trends For 2021 that Hybrid will be declared the Winning Enterprise Architecture with more choice in workload locations. In the fullness of time, the public cloud will itself migrate to the edge. This shift will become known as ‘distributed cloud’ and will ultimately need to be automated and possibly even become autonomous.

Security & Sovereignty

This will take centre stage as Australia seeks to protect itself from cyber risks and malicious state actors. Domestic storage, security and controls will increase in importance as agencies seek to preserve IP and protect citizen and critical infrastructure data and access.

There are very few teams that are not aware of the essential-8 requirements to mitigate cyber security incidents. Of particular interest is how security plays out in backups and recovery. The last defence against ransomware infections and other attacks will always be backup. In the event of a ransomware attack, infected systems can be taken offline and revert to the last clean system copy for restoration.

While this is an overly simple scenario; in practice, security teams will need to work closely with infrastructure to determine the genuine clean system copy. Under the pressure to recover it can be easy to make assumptions and re-install the malware or not close out malicious backdoors - only to be re-compromised. A backup infrastructure that is prepared, practiced and scaled has never been more important than today.

TECHNOLOGY LAYER	SOFTWARE AS A SERVICE (SAAS)	PLATFORM AS A SERVICE (PAAS)	INFRASTRUCTURE AS A SERVICE (IAAS)
People	Agency	Agency	Agency
Data	Agency	Agency	Agency
Applications	Cloud Service Provider	Agency	Agency
Operating System	Cloud Service Provider	Cloud Service Provider	Agency
Virtual Networks	Cloud Service Provider	Cloud Service Provider	Agency
Hypervisors	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Servers and Storage	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Physical networks	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider

Clarification on security responsibilities is also crucial. NSW proposed responsibilities are as per the table [*1]

Importantly, GovDC will introduce colocation services certified to PSPF Zone 3.
This will enable support of Government systems or workloads classified to **protected** level.

[1] NSW Government Cloud policy, September 2020, page 14

Part 2: Research insights

To better understand these trends and some of the perceptions of agencies, recent research conducted in NSW in August 2020 found the following:

Current perceptions and understanding across multiple layers of Government (State, Independent, Local Govt) of GovDC and its important role in Government.

There appears to be a broad understanding of GovDC, the value it has delivered and its mission. Its approach to the next phase is understandably less clear with the recently released cloud strategy and policy. This could be because IT teams will need to consider which workloads are suitable for public, private, secure and edge clouds. Agencies are increasingly adopting distributed cloud approaches for different workloads based on their particular data, performance, cost and security needs.

Unmanaged this has the potential to create a lot of variability in the operating models. The general view was that complexity would be increased but this could be offset with standardised patterns, programmable infrastructure, serverless models and automation.

GovDC has ambitions for Local Government (which are well founded) but until Edge is applied to the portfolio it may be constrained by the reluctance of Local Government (outside of metropolitan Sydney) to relocate all infrastructure to metro/ Sydney or to become completely dependent on remote services. This is heavily driven by the cost and performance of backhaul bandwidth. Many councils have not invested heavily in disaster recovery and business continuity capabilities which will drive edge and GovDC compute and storage. It is a real opportunity for Councils to dramatically lift their resilience and security posture.

COVID-19 has changed agency plans and approaches

Everyone that was interviewed acknowledged the massive impact that COVID19 has had. Not just to the operational shift to working from home but by the recognition of the importance of IT in enabling any agency to operate in the new normal.

IT finally has a seat at the table rather than being relegated to the back end of Government.

One thing weighing heavily on the minds of many is current networks and infrastructure is orientated toward work from office whereas it is unlikely that things will ever return to where they were. Many permanent architectural and re-balancing decisions will need to be made soon as the new normal becomes normal.

Leaders are not just wrestling with the technical aspects but the human aspects of teams, collaboration, home-workplaces etc.

What priorities exist for clusters and agencies regarding GovDC?

All the agencies interviewed had some sort of footprint in GovDC. Their priorities varied greatly from a business perspective but there were strong interests around hybrid options with public cloud first and fit for purpose edge configurations. Almost everyone wanted flexibility and security was at the forefront of everyone's minds.

Understandably not everyone was completely up to date on the recent cloud developments with GovDC and some agencies raised concerns around understanding the interconnectedness of cross agency security and data. That is, what services are connected to which services? The same agencies also expressed a desire to see some sort of cross agency governance when these services are interconnected.

Imperatives that exist regarding moving to a GovDC environment or a GovDC managed service

Apart from solution fit and the cost efficiency of solutions; security features very strongly. Agencies were interested not just in the service that was being delivered but who these services were contracted out to (e.g. offshore) and sovereignty, governance and location of data were high on the agenda.

There were differing views on whether GovDC should involve itself in ensuring the quality of Marketplace solution or if this should be left to the agencies taking up these services.

Almost all interviews recognised that public cloud would play an ever-increasing role, but workloads would be orientated to the problem being solved. 'One size fits all' usage would decrease in popularity driving distributed compute and storage.

Recent security, data and geopolitical events have changed thinking and attitudes

- Security and the Geo-political consequences are causing a review of attack surface and posture
- Cyber and Data security sensitivities are elevated. State-based actors have changed the landscape irrevocably.
- COVID-19 has impacted priorities and operating models. New WFA (Work from Anywhere) will replace Work from Home. Temporary arrangements for COVID-19 will give way to permanent workforce changes. This will change the services that agencies require and the demand they will have from their staff and customers.

Conclusions and next steps

The requirement for all agencies to develop cloud strategies and transition plans - and then submit them to the ICT and digital leadership group by July 2021 is explicit. This requires deep consideration of the future and anticipation of the changes and expectations that are upon the public sector.

To this end, successful IT leaders and infrastructure teams are advised to:

- Engage partners (i.e. service providers) who are focused and agile enough to provide solutions oriented to the problem being solved using fit for purpose offerings and technology.
- Start early - there is much to be done and many stakeholders to collaborate with. Digital, data and security teams will be empowered or constrained by the decisions that are made.
- Prepare for the inevitability of digital transformation to public cloud.
- Prepare for massive amounts of data generated by IoT and sensors powered by 5G
- Understand the real-time and AI requirements of the next generation of applications and services for citizen services.
- Understand and match workload locations to the outcomes that are required - security, cost, performance and scale. There are opportunities to maximise this in GovDC and at the edge with distributed public or private cloud.
- Change operational processes when migrating workloads to public cloud to ensure that consumptive costs are managed, and bill shock is avoided or reduced. Orchestrate and automate if you can; and invest time in defining your patterns.
- Keep more data onshore and elevate attention to privacy and security controls.
- Use AI, compute and storage as close to where it will be used as possible to drive down network bottlenecks and user/application experience.
- Review existing 'one size fits all' strategies in favour of optimised strategies.
- Review security posturing for distributed data, public, distributed/hybrid cloud as well as the proliferation of WFA (work from anywhere).

IT finally has a seat at the table. COVID-19 has brought IT closer to its internal customers and business units than ever before. It has demonstrated its criticality in keeping the Government operational and tangibly impacted every employee and citizen in some way.

By leveraging this new level of credibility and the trusted relationships forged in responding to COVID-19 the value and relationships established in batting the pandemic will be consolidated.

There is no doubt that the future for Government will be more secure, scalable and sovereign. There will be increased use of public and flexible (distributed/hybrid/edge) workloads to service the next generation of applications and security needs of the Government. NSW has demonstrated significant leadership in laying out its strategies and policy with such clarity and purpose.

About the Author:

Ian Jansen is a PSN Advisor and former Chief Digital & Product Officer in Government and the private sector. Ian has worked at Dimension Data (NTT), LinkedIn and the NSW Government. Most recently Ian co-founded a start-up called Lassio that delivers automation and AI at scale and as a service. During his time in the public sector Ian led the first NSW Government end-to-end public cloud migration into public cloud.

About PSN:

Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. It and develops roundtables, seminars, and conferences to suit current areas of interest to government agencies and their suppliers.

PSN's growing community spans across federal, state, and local government departments, healthcare, and education, allowing members to share information, access the latest in government innovation, and engage with other like-minded individuals on a secure and closed-door network.

PUBLIC SECTOR NETWORK

About the sponsors:

Australian MSP, Secure Agility has developed a secure, enterprise and government-grade cloud platform with partners Cisco, Rubrik and Pure Storage.

OurDC4 is a collaboration of these four partners that delivers a modern data centre-as-a-service for customers across three geographically diverse, Tier 3 data centres in NSW. Public and private cloud compatible, this includes residing within NSW GovDC, meaning it is sanctioned for use by NSW State government departments as part of its digitisation push.

For more information see
https://secureagility.com/ourdc4/

OurDC 4
GovDC to the power of 4

cisco Partner · PURESTORAGE · rubrik · SECURE AGILITY

Network and Security Assessment offer:

Remember that the NSW State Government requires all agencies to submit their cloud strategy and transition plans by July 2021. Knowing your current network and security status is a good place to start building this picture.

Our Essential Detection Starter package will address at least half of the Essential 8 areas of criticality. Highlight your risk profile with this package that includes Discovery, Analysis and Reporting. **Learn more here:**

For further information please contact:

www.secureagility.com
inform@secureagility.com
LinkedIn #thepowerof4