NSW Government Cloud Policy

Author: Department of Customer Service
Version number: v1.1
Date: Wednesday, October 07, 2020

The NSW Government Cloud Policy will be reviewed in twenty-four months from the issue date, or earlier in response to post-implementation feedback from agencies.

Contact details

Contact: Department of Customer Service, ICT and Digital Sourcing
Email: ICTServices@customerservice.nsw.gov.au

October 2020

Table of Contents

1. Introduction

The NSW Government is making the strategic shift to cloud consumption through the use of public and private cloud services. The NSW Government Cloud Policy provides guidance and direction to NSW Government agencies in making use of public and private cloud services.

NSW Government agencies must use this policy to ensure their consumption of cloud services is efficient, secure, and financially sound. In doing so, this policy will enable alignment, consistency, optimal commercial outcomes, reduced risk, and improved delivery of services to citizens across the NSW Government.

The NSW Government Cloud Policy must be used by NSW Government agencies in understanding the available cloud services, determining the appropriate future usage of cloud services as well as procuring and securing cloud services appropriately.

The NSW Government Cloud Policy is presented in six sections:

1. **Introduction**: outlines background and context, introduces what this policy is, the outcomes to be achieved by following this policy, the scope of the policy and NSW Government agency responsibilities in following the policy.
2. **Cloud Services**: defines the public and private cloud services available to NSW Government and outlines the benefits of consuming cloud services.
3. **Cloud Service Selection**: provides guidance on selecting cloud services including workload assessment considerations.
4. **Cloud Service Procurement**: provides alignment to the existing procurement policies and procurement guidance including through buy.NSW and NSW Government cloud contracts.
5. **Cloud Security**: provides alignment to the Cyber Security Policy and identifies relevant security obligations in consuming cloud services.
6. **Appendix**: provides context on the development of this policy and further resources to guide agencies in their adoption and consumption of cloud services.

1.1 Background and Context

The NSW Government's ICT and Digital landscape has evolved significantly over the last decade through delivery of the NSW Government Data Centre Reform and growth in the consumption of cloud services.

The NSW Government has continued to increase ICT service offerings through the introduction of GovDC, implementation of dedicated cloud network connectivity, development of the private cloud marketplace, and introduction of mechanisms to support access to public cloud services. In parallel, NSW Government agencies have been increasing their consumption of public cloud services to support responsive delivery of innovative and scalable services to the citizens of NSW.

Due to the large range of NSW Government agency use cases for IT services and the need to balance legacy IT systems with more responsive delivery of contemporary services, the NSW Government ICT and Digital landscape has evolved to utilise both public and private cloud platforms.

The NSW Government Cloud Policy combines the previous cloud and data centre policies to enable secure, efficient, and financially sound consumption of public and private cloud services. This policy was developed in collaboration with all NSW Government Clusters, to bring real world relevance on how the NSW Government agencies are consuming and planning to consume cloud services into the future.

1.2 What is the NSW Government Cloud Policy?

This policy aligns and modernises the Cloud Policy (2018), GovDC page (2018), and Data Centre Reform Circular (2018) by consolidating them into a single policy. It provides linkage to the Beyond Digital Strategy and and NSW Government Cloud Strategy by aligning to the desired outcomes of both strategies. Furthermore, this policy will guide NSW Government agencies in their adoption and consumption of cloud services by incorporating the latest changes in the technology, procurement and cyber security landscapes.

The NSW Government Cloud Policy provides guidance and recommendations on the consumption of public and private cloud services. The NSW Government Cloud Policy is ‘public cloud first’ meaning NSW Government agencies must make use of public cloud services as the default. Where public cloud services are not suitable for agency requirements, private cloud services, provided through the Government Data Centres (GovDC) can be used by exception.

The consideration for selection of cloud services is detailed in section 3.

1.3 Policy Outcomes

The NSW Government Cloud Policy provides guidance and direction to enable NSW Government agencies to achieve the following outcomes:

Security – adhering to this policy guidance, regarding usage of cloud services will ensure NSW Government agency assets and data are secured.

Consistency – NSW Government agencies receive common direction in the consumption of cloud services, allowing them to make consistent usage of the public and private cloud services.

Modernisation – the NSW Government Cloud Policy guides NSW Government agencies in consuming cloud services to modernise their ICT and Digital service delivery. The policy enables modernisation through lineage to updated business processes for procurement, security, and consumption of cloud services.

Alignment – By defining and guiding the usage of cloud services, this policy ensures alignment of cloud service consumption across the NSW Government in accordance with NSW Government strategic objectives and priorities.

Innovation – enables NSW Government agencies to consume new cloud capabilities such as AI, machine learning, data analytics etc. By leveraging cloud services, the NSW Government will be able to keep up with services released by industry, without having to build and maintain each capability.

Optimal Commercial Outcomes – NSW Government agencies will contribute to optimising NSW Government commercial outcomes by using strategic partnerships with public cloud services providers, whole of government agreements and purchasing arrangements that have been established and referred to in this policy.

1.4 Scope & Responsibility

The NSW Government Cloud Policy applies to all NSW Government clusters and agencies. It does not apply to State Owned Corporations, but it is recommended for their adoption.

All NSW public sector Secretaries and Chief Executives are responsible for ensuring that this policy is applied within their clusters and/or agencies. It is also recommended that compliance is regularly reviewed by each agency's Risk and Audit Committee. The NSW Government ICT and Digital Leadership Group (IDLG) provides oversight for this policy.

2. Cloud Services

This section of the policy defines cloud services available to NSW Government and identifies the benefits of consuming cloud services.

The following cloud services are available to NSW Government agencies:

- **Public Cloud:** Public cloud services are operated by third party cloud service providers, who own, manage, and deliver computing resources (e.g. compute, storage) over the internet. These computing resources are delivered to multiple organisations.
- **Private Cloud:** The NSW Government provides private cloud services through GovDC managed and operated data centres.
- **Dedicated Network and Cloud Connectivity:** The NSW Government private cloud offers dedicated network interconnects between private cloud services and public cloud services.

The diagram below depicts the cloud services available to NSW Government.

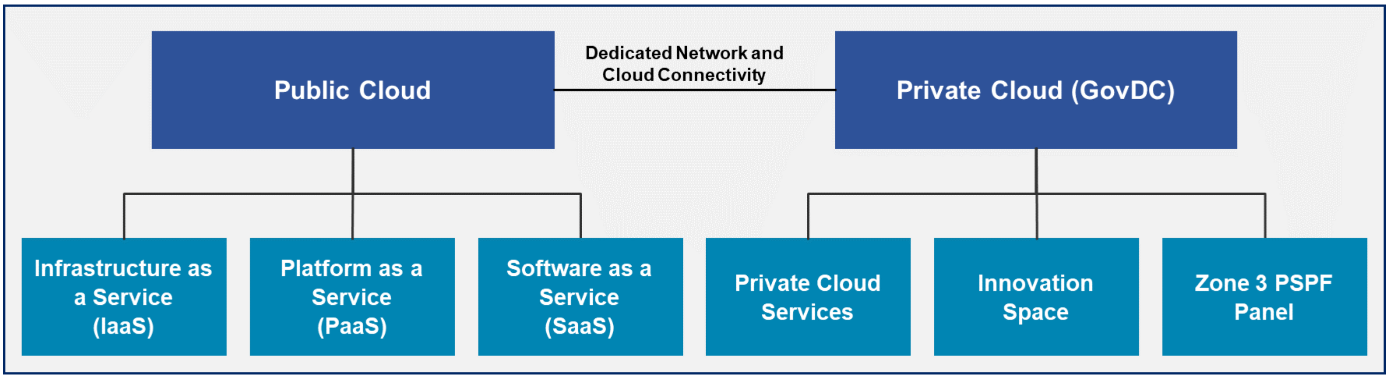

Public Cloud
Dedicated Network and Cloud Connectivity
Private Cloud (GovDC)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Private Cloud Services
Innovation Space
Zone 3 PSPF Panel

Figure 1 - NSW Government Cloud Services

2.1 Public Cloud Services

Public cloud services are highly diverse, with varying models for consumption. The types of services that can be consumed through public cloud include:

- **Infrastructure as a Service (IaaS)**: Consumption of ICT infrastructure (server, storage, network, operating system) from a cloud provider. Resources are consumed on demand for as long as they are needed.
- **Platform as a Service (PaaS)**: Consumption of ICT platform to allow for the development, operation, and management of applications without the complexity of building and maintaining infrastructure.
- **Software as a Service (SaaS)**: On demand delivery of software applications, with cloud providers hosting and managing the application and its underlying infrastructure.

Public cloud services are consumed through global hyperscale providers such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) as well as Australian providers such as Vault and Macquarie Government (to name a few). Each cloud provider has differing areas of focus, maturity, and speciality. A list of Government approved cloud services can be found on buy.nsw.

The NSW Government Procurement Policy Framework outlines the steps to source cloud services which are further detailed in section 4 Cloud Service Procurement.

2.2 Private Cloud Services

Private cloud services enable NSW Government agencies to consume ICT infrastructure in a highly efficient manner with a high standard for physical security. Private cloud services are delivered through the GovDC managed and operated data centres that were built in 2012. These services have evolved to meet the changing needs of NSW Government agencies.

Private cloud services include the following:

1. Private Cloud

Private cloud offerings refer to cloud computing resources used exclusively by a single organisation, with services and infrastructure maintained on a private network. Where an NSW Government agency has taken the position to consume their infrastructure as a service, they may engage a vendor to build a dedicated environment, within GovDC managed and operated data centres, on their behalf.

2. Community Cloud

The community cloud (marketplace) is a secure environment for the provision of as-a-service solutions from a growing number of vendors, dedicated to NSW Government agencies. NSW Government agencies can acquire services through the ever growing ICT Services Catalogue, or by contacting the private cloud team at GovDC@customerservice.nsw.gov.au

3. Dedicated Network and Cloud Connectivity

NSW Government private cloud facilities are supplier neutral and are open to all cloud service providers to offer cloud connectivity. A comprehensive array of suppliers is already on board. This service provides:

- Access to dedicated Hyperscaler network links
- Services supplied by AARNet for academia and associated entities.

To access any of the approved NSW Government cloud services, go to buy.nsw.

Suppliers that offer services through the NSW Government private cloud are included on buy.NSW but must be procured following the requirements and considerations detailed in section 4 Cloud Service Procurement.

4. Innovation Space

The Innovation Space is an incubator to develop a broader catalogue of private cloud services. By lowering the commitment and investment required, the Innovation Space encourages cloud service providers to build demonstration and test environments of their offerings and latest technologies for NSW Government agencies. After successfully proving their offering and entering a commercial arrangement with a tenant, the offering then transitions into the private cloud.

5. Zone 3 PSPF Panel

In September 2020, GovDC will introduce colocation services certified to PSPF Zone 3. This will enable support of Government systems or workloads classified to PROTECTED level. For more information on Data Classification standards, refer to section 5.c. Data Classification.

6. Cloud Advisory and Procurement

The Technology Services program can support agencies in the procurement and deployment of cloud services through advisory and management services.

For more information on private cloud services, please contact GovDC@customerservice.nsw.gov.au.

2.3 Cloud Benefits

Cloud services continue to enable transformational opportunities across NSW Government operations, enabling the delivery of citizen focused services anywhere, anytime, through the following benefits:

- **Interconnected Ecosystem:** The NSW Government private cloud currently hosts the majority of NSW Government agency ICT infrastructure, making it the launchpad for agencies looking to connect existing systems or workloads to public cloud services through dedicated network connectivity
- **Collaboration**: As a community of NSW Government agencies, the NSW Government private cloud facilitates collaboration and sharing that is difficult to achieve when ICT and Digital service delivery is distributed
- **Rapid Elasticity:** The on demand model of Cloud allows NSW Government agencies to rapidly scale up and down their infrastructure in line with end user and developer needs, allowing the NSW Government to keep up with growing and changing citizen demands
- **High Availability:** ICT services running in the cloud can be architected to be highly available and resilient, ensuring fewer outages and less down time by leveraging constructs such as availability zones and autoscaling.
- **Access to New Capabilities:** Cloud services provide the NSW Government the foundations upon which to deploy more advanced capabilities such as artificial intelligence and machine learning, as well as access to continual updates and service improvements
- **Flexibility:** By consuming cloud services, the NSW Government will have access to a range of programming models, operating systems, databases, and architectures as well as supplier services available through marketplaces provided by the public cloud services providers
- **Automation:** Platform and application automation can enable greater ease of management across ICT environments as well as self service provisioning capabilities
- **Focus on Service Differentiation:** Cloud consumption enables NSW Government agencies to transition away from the undifferentiated heavy lifting of managing infrastructure by consuming it as a service, allowing greater focus on transforming services for citizens

- **Greater Security and Resiliency:** Cloud environments can be configured to track changes using logging and can make use of the latest security features to reduce the likelihood of cyber-attacks and internal misconfiguration
- **Cost Avoidance:** Cloud services enable the NSW Government to pay for resources used, on demand. This can enable upfront cost avoidance on infrastructure refresh and long term cost savings as workloads are optimised in the cloud environment
- **Business Agility:** Cloud services support more agile development and deployment practices, which can significantly reduce time to market if processes are updated to make use of rapid provisioning
- **Centralisation and Visibility:** Strong governance of cloud services can help to centralise ICT environments and provide clearer visibility of consumption and costs.

Whilst the benefits listed above are achievable through both public cloud and private cloud, they are more attainable through public cloud. Public cloud service providers have developed the tools, commercial constructs, and services for Government agencies to architect, configure and govern cloud services to realise these benefits.

3. Cloud Service Selection

NSW Government agencies can consume public and private cloud services. This section will provide guidance on the selection of cloud services including making cloud service decisions and the considerations that will influence service selection.

3.1 Making Cloud Service Decisions

NSW Government agencies must consider the four lenses of Strategy, Policy, Procurement and Cyber Security to inform their cloud service decisions.

Strategy Lens – is driven by the Beyond Digital Strategy, NSW Government Cloud Strategy, and agency cloud strategies. These strategic drivers state:

- The Beyond Digital Strategy states that NSW Government agencies must be shifting efforts from running ICT to transforming customer services
- The NSW Government Cloud Strategy states agencies must 'Enable government-wide adoption of public cloud services in an aligned and secure manner, to accelerate innovation, modernise service delivery and drive better outcomes for the citizens of NSW'
- Agencies must develop their own cloud strategies and transition plans and submit these to the NSW Government ICT and Digital Leadership Group by 30th June 2021.

Policy Lens – is driven by the NSW Government Cloud Circular and NSW Government Cloud Policy. These policy drivers state:

- All NSW Government agencies must make use of public cloud services as the default. Where public cloud services are not suitable for agency requirements, private cloud services, provided through the Government Data Centres (GovDC) can be used by exception
- The use of public cloud services will apply to new agency ICT services and the material replacement or renewal of any existing services, platforms, and infrastructure
- Exemptions to the use of public cloud services will be reviewed in cases where public cloud services are not suitable, as assessed through one or more of the following pre-requisites: cost-benefit analysis, market scan of public cloud services, or security assessment
- In cases where ICT services cannot be consumed through public cloud, agencies will be required to develop a briefing paper to request exemption, supported by these pre-requisite assessments

- Exemption requests that are associated with a funding submission to the Digital Restart Fund will be reviewed and approved by NSW Government Delivery and Performance Committee (DaPCo), and are to be submitted in conjunction with the Delivery and Performance Architecture (DAPA) checklist
- Exemption requests that are not associated with a funding submission to the Digital Restart Fund will also be reviewed and approved by DaPCo and are to be submitted in conjunction with the bi-monthly ICT assurance, cyber and procurement DaPCo submission
- Agencies must operate all private cloud services through GovDC.

Procurement Lens – is driven by the NSW Government Procurement Policy Framework, NSW Procurement Board Direction and NSW Government agreements with cloud service providers. These procurement drivers are:

- The Procurement Policy states that agencies 'must evaluate cloud-based services when procuring ICT goods and services. The evaluation must be based on cost-benefit analysis and achieving value for money over the life of the investment.'
- NSW Government agencies must make use of mandated Whole of Government Agreements (where they exist)
- Where no NSW Government agreements exist, agencies must use the relevant ICT Procurement contract framework to source ICT services.

Cyber Security Lens – is driven by NSW Cyber Security policy, relevant legislative requirements (further explored in section 5 of this policy) and agency specific security plans. The cyber security drivers are:

- Agencies must meet cyber security requirements outlined in the NSW Cyber Security Policy
- Agencies must consider the protective marking of their data and implement security mechanisms that meet these data classification requirements.

3.2 Workload Considerations

There are several prompts that signal when NSW Government agencies must consider their ICT platform or service consumption options. These include:

- there is a major equipment/infrastructure refresh due;
- there is a major software refresh due;
- there is an emerging defined need for cross agency connectivity;
- there is an opportunity to consume an application through software as a service, or consolidate applications across agencies or a cluster;
- existing solutions do not meet agency, staff or customer needs; and
- systems have limited support from staff or suppliers or are becoming increasingly difficult to support.

When a NSW Government agency is seeking a new platform or service consumption option, they must consider the following factors:

- **Accessibility**: Cloud services must be accessible to WCAG 2.0 AA or above
- **Capabilities**: NSW Government agencies may have a need for specific capabilities (e.g. artificial intelligence, machine learning) which require the consumption of certain cloud services
- **Cost-Benefit**: An analysis must be conducted on the costs and benefits of moving a workload to a specific cloud service. Assessment must include value for money, fitness for purpose, a clearly defined business case (with benefits realisation reporting), the total cost of ownership (TCO), asset impact, organisational impact, and technical environment impact
- **Technical and Network Requirements**: With considerations such as enterprise architecture, bandwidth, response time, capacity, priority, availability, firewalling, automation, virtualisation, compatibility, interoperability, and configuration
- **Risk Management**: NSW Government agencies must undertake comprehensive risk assessments, including on network access, storage and maintenance of data or information and records held by third parties or suppliers
- **Cyber Security**: The agency must ensure that the management of the cloud service provider meets the security obligations as defined in the NSW Cyber Security Policy
- **Skillsets**: The ability of the NSW Government agency team to support the cloud service/s

- **Privacy**: Ensure the cloud service provider meets NSW information privacy laws and any other applicable privacy laws including:
  - *Privacy and Personal Information Protection Act 1998* (PPIPA)
  - *Government Information (Public Access) Act 1998* (GIPA)
  - *Health Records and Information Privacy Act 2002* (HRIPA)
- **Ownership**: The NSW Government must retain ownership and control of all consumer data from the time it is created, and cloud service providers are not permitted to access or use any consumer data for purposes other than specified in the contract between the NSW Government agency and the cloud service providers
- **Insurance**: Cloud service providers should be appropriately insured including for public liability, product liability, workers' compensation, cyber security, and professional indemnity. For further detail of the insurance requirements refer to the relevant ICT Procurement contract frameworks
- **Jurisdiction**: contracts should nominate NSW as the exclusive jurisdiction of the agreement, including for any disputes. The *State Records Act 1998* is the primary consideration regarding the creating, management, protection and ongoing accessibility of records of public offices in NSW. Sending records for storage with, or maintenance by, suppliers based outside of NSW is permitted – provided that an appropriate risk assessment has been conducted, and records are managed in accordance with all the requirements applicable to State records.

4. Cloud Service Procurement

As NSW Government agencies determine the appropriate mix of cloud services to suit their needs, they will need to undergo procurement activities to source these cloud services. Procurement of cloud services is governed by the NSW Procurement Policy Framework and NSW Procurement Board Direction.

This section will outline cloud service procurement considerations, the role of buy.NSW as well as sourcing and contracting considerations.

4.1 Procurement Requirements and Considerations

The Procurement Policy Framework outlines the procurement process (Plan, Source and Manage). Buy.NSW providers guidance on navigating the procurement process including:

- Plan: Best practices including when and how to approach the market;
- Source: Finding the right supplier, going to market, and awarding the contract; and
- Manage: Fostering a relationship so suppliers can excel while meeting obligations.

The following are procurement requirements and considerations for cloud services:

- Agencies must use the ICT Services Scheme. The scheme offers a panel of prequalified suppliers to provide a range of ICT solutions to assist NSW Government agencies and other authorised buyers
- Agencies should leverage buy.NSW, which provides a supplier list for initial market analysis. The supplier list is not exhaustive, with new suppliers continuing to be onboarded to the platform
- Agencies must develop a business case and funding request, inclusive of a value for money assessment, which must include consideration for cloud offerings, where appropriate
- Agencies should apply to funding from the Digital Restart Fund (DRF). The purpose of the DRF is to accelerate whole of government digital transformation. Cloud initiatives may be eligible for the following DRF initiative categories:
  - State digital assets: solutions that create cost savings and consistent user experience through increasing agencies' use of core and common ICT components
  - Legacy modernisation: initiatives that support agency digital innovation, ICT modernisation, and reuses State Digital Assets

4.2 buy.NSW

buy.NSW is designed for NSW Government to make informed decisions when buying goods and services. It offers a space for buyers and sellers of products and services to connect and do business.

- Buyers can search for, identify, and contact suitable suppliers; and
- Suppliers can register to do business with government, manage their profile and provide information on their goods and services.

4.3 Sourcing & Contracting

The NSW Procurement Board Direction states that NSW Government agencies must use whole of government contracts for obtaining the goods or services to which those contracts apply, except where specific exemptions are provided by Procurement Board policies. These contracts must be used, where they provide the best value for money, as determined through an assessment of the cloud consumption over the life of the contract. Where cloud consumption changes, these contracts, and their use, must be re-evaluated.

The list of whole of government contracts can be found on buy.NSW.

Where a suitable whole of government contract does not exist, agencies must use one of the following Procure IT Framework components:

- Core& Contracts – may be used for low risk procurements with a contract value up to $1,000,000 (excl. GST); or
- Procure IT v3.2 – for all high risk procurements with a contract value over $1,000,000.

The Department of Customer Service has also developed a new form of agreement for IaaS and PaaS termed the Digital.NSW Cloud Framework Agreement. This agreement is currently being used as the basis for the Cloud Purchasing Arrangements (CPA) and will be incorporated into future revisions of ProcureIT. The Digital.NSW Cloud Framework Agreement may also be made available in future as an alternative to ProcureIT v3.2 and Core& subject to approval by the Procurement Board. Further information on the CPA is outlined below.

4.4 Cloud Purchasing Arrangements (CPA)

In 2019 the Department of Customer Service commenced development of the CPA. The CPA is a collection of whole of government contracts which are available for consumption of cloud services, generally via the public cloud and community cloud deployment models. The CPA has been developed primarily to address forecast growth in demand for IaaS and PaaS but may also facilitate consumption of other service types including professional services, hosted security services and software as a service depending the specific contract.

A CPA whole of government contract typically incorporates a commercial framework providing a range of benefits to buyers in recognition of whole of government volume. It also enables suppliers to provide a compelling and standardised offer to eligible buyers, enabling transactions to be streamlined.

Benefits to buyers vary from contract to contract depending on volume, seller and the nature of services offered. Benefits may include:

- discounts off cloud services generally expressed as a percentage reduction off government list prices,
- training and migration offers,
- enhanced support offerings,
- onsite technical support at reduced cost and
- discounted professional services including cloud strategy, planning and migration support.

CPA whole of government contracts are standing offers where buyer will enter a customer contract (or equivalent) under a head agreement before raising orders. It is therefore important that each buyer assess and can demonstrate value for money associated with their preferred suppliers prior to raising orders.

CPA contracts also take one of three forms:

1. an amendment of an existing whole of government contract to accommodate cloud services
2. variation of a contract available through another jurisdiction such that it is suitable for use by NSW buyers or
3. a new contract based on the Digital.NSW Cloud Framework Agreement.

CPA whole of government contracts, including scope and details of applicable benefits, will be published on buy.nsw as they are approved.

5. Cloud Service Security

NSW Government agencies must abide by the NSW Cyber Security Policy when protecting services and data hosted using cloud services. This section will help agencies identify the technology layers they are responsible for security, their security obligations as well as security requirements based on data classification.

5.1 Security in the Cloud

Securing data in the Cloud is a shared responsibility between NSW Government agencies and their cloud service providers. The cloud service provider is responsible for security 'of the Cloud', whilst agencies are responsible for security 'in the cloud'. The table below outlines the delineation of this responsibility across cloud consumption models:

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

Agencies should refer to the table above to understand the technology layers they are responsible for securing and refer to the NSW Cyber Security Policy to understand the requirements and considerations to apply across each of these areas.

5.2 Security Requirements and Considerations the Cloud

The NSW Cyber Security Policy outlines mandatory requirements to appropriately manage cyber security risks including:

- Conduct cyber security risk assessments and include identified risks in the NSW Government agency's overall risk management framework
- Agencies remain accountable for the cyber risks of their ICT suppliers and ensure the suppliers also comply where relevant, including notification of security incidents
- Agencies must implement regular cyber security education for all employees, contractors, and outsourced ICT service providers
- Agencies must have any crown jewel systems at a minimum covered by a Cyber Security Framework (CSF) or Information Security Management System (ISMS) compliant with, or modelled on an appropriate commonly used standard (E.g. ISO27001) Cyber Security requirements are built into the procurement process and into the early stages of projects and the system development life cycle (SDLC) including agile projects.
- Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data, including processes for internal fraud detection.

The Australian Cyber Security Centre's Cloud Computing Security Considerations provide detailed security considerations, applicable to cloud services, which include:

1. Maintaining availability and business functionality
2. Protecting data from unauthorised access by **a third party**
3. Protecting data from unauthorised access by **the supplier's customers**
4. Protecting data from unauthorised access by **rogue supplier employees**

5.3 Information Classification, Labelling and Handling

The NSW Government Information Classification, Labelling and Handling Guidelines detail how NSW agencies can correctly assess the sensitivity and security of their information, label and then handle this information safely. These guidelines align closely with the Commonwealth Protective Security Policy Framework (PSPF).

The PSPF has been updated in 2018. The PSPF has three security classifications, PROTECTED, SECRET and TOP SECRET. The PSPF can be found here.

Protective Marking	Business Impact Level	Compromise of information confidentiality would be expected to cause:	Personnel security clearance for ongoing access
PROTECTED	High business impact	Damage to the national interest, organisations, or individuals.	Baseline security clearance or above.
SECRET	Extreme business impact	Serious damage to the national interest, organisations, or individuals.	Negative Vetting 1 security clearance or above.
TOP SECRET	Catastrophic business impact	Exceptionally grave damage to the national interest, organisations, or individuals.	Negative Vetting 2 security clearance or above.

The NSW Government Information Classification, Labelling and Handling Guidelines are currently being updated to be consistent with the PSPF. The NSW Cyber Security Policy requires agencies to adhere to the new NSW Guidelines.

6. Appendix

6.1 Policy Development

The NSW Government Cloud Policy has been developed with inputs from the NSW Government Cloud Strategy, the existing policy landscape and stakeholder feedback from agencies with experience in navigating the existing policy documents.

NSW Government Cloud Strategy

In late 2019, all eight NSW Government Clusters were engaged to align on a vision for cloud consumption within the NSW Government. IT leaders across all clusters and a representative sample group of cloud service providers were engaged to understand the supply and demand side challenges for consuming cloud services within the NSW Government.

The strategy identified the need for mechanisms to support procurement, security, funding, and talent. This updated policy addresses some of the procurement and security considerations in section 4 Cloud Service Procurement and section 5 Cloud Service Security.

For further information, the NSW Government Cloud Strategy can be found here.

Existing Policy Landscape

The existing policy landscape for cloud and GovDC were reviewed as part of the analysis for the NSW Government Cloud Policy. This analysis identified 12 existing documents, developed between 2014 and 2020, that provide guidance on consumption of public and private cloud services. This set of policy documents has contributed to a complex policy environment that was difficult for NSW Government agencies to navigate and effectively consume in support of service delivery.

The diagram below depicts the various active documents and the relationships between them:

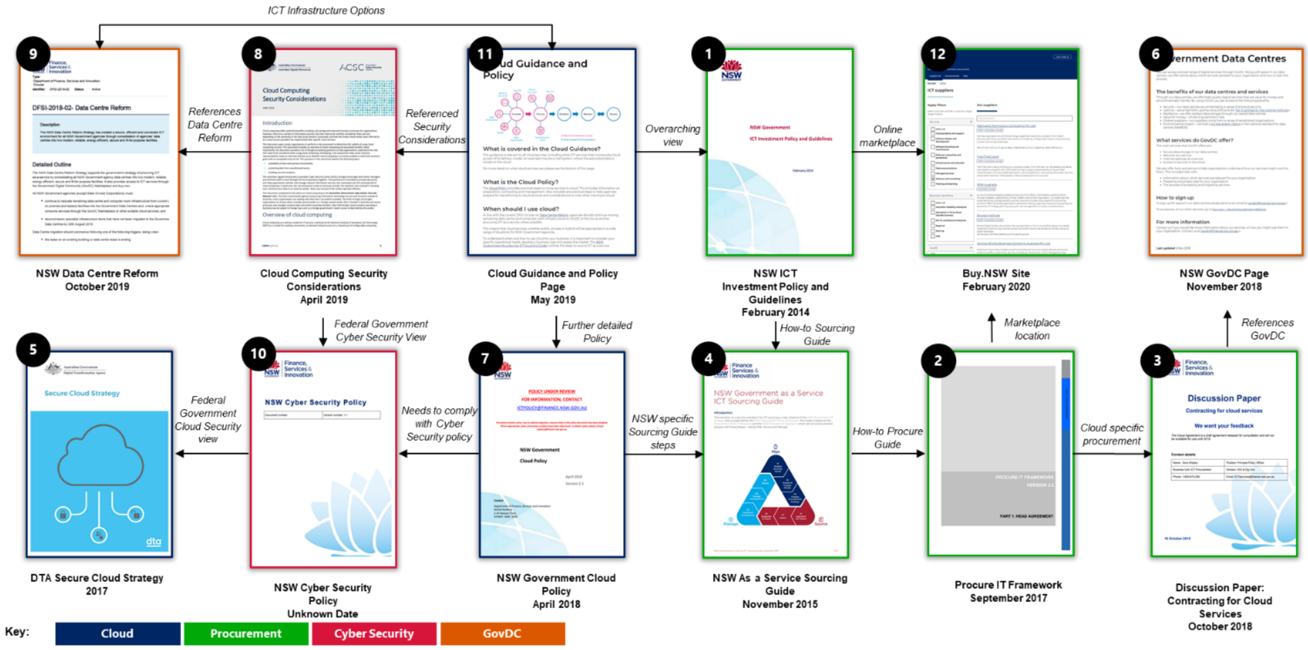

ICT Infrastructure Options
9
NSW Data Centre Reform
October 2019
References Data Centre Reform
8
Cloud Computing Security Considerations
April 2019
Referenced Security Considerations
11
Cloud Guidance and Policy Page
May 2019
Overarching view
1
NSW ICT Investment Policy and Guidelines
February 2014
Online marketplace
12
Buy.NSW Site
February 2020
6
NSW GovDC Page
November 2018
Federal Government Cyber Security View
Further detailed Policy
How-to Sourcing Guide
Marketplace location
References GovDC
5
DTA Secure Cloud Strategy
2017
Federal Government Cloud Security view
10
NSW Cyber Security Policy
Unknown Date
Needs to comply with Cyber Security policy
7
NSW Government Cloud Policy
April 2018
NSW specific Sourcing Guide steps
4
NSW As a Service Sourcing Guide
November 2015
How-to Procure Guide
2
Procure IT Framework
September 2017
Cloud specific procurement
3
Discussion Paper: Contracting for Cloud Services
October 2018
Key:
Cloud
Procurement
Cyber Security
GovDC

Figure 2 - Complex Policy Landscape for Navigating Cloud and GovDC

The relevant existing policies were reviewed in detail to understand components to be incorporated in this Cloud Policy.

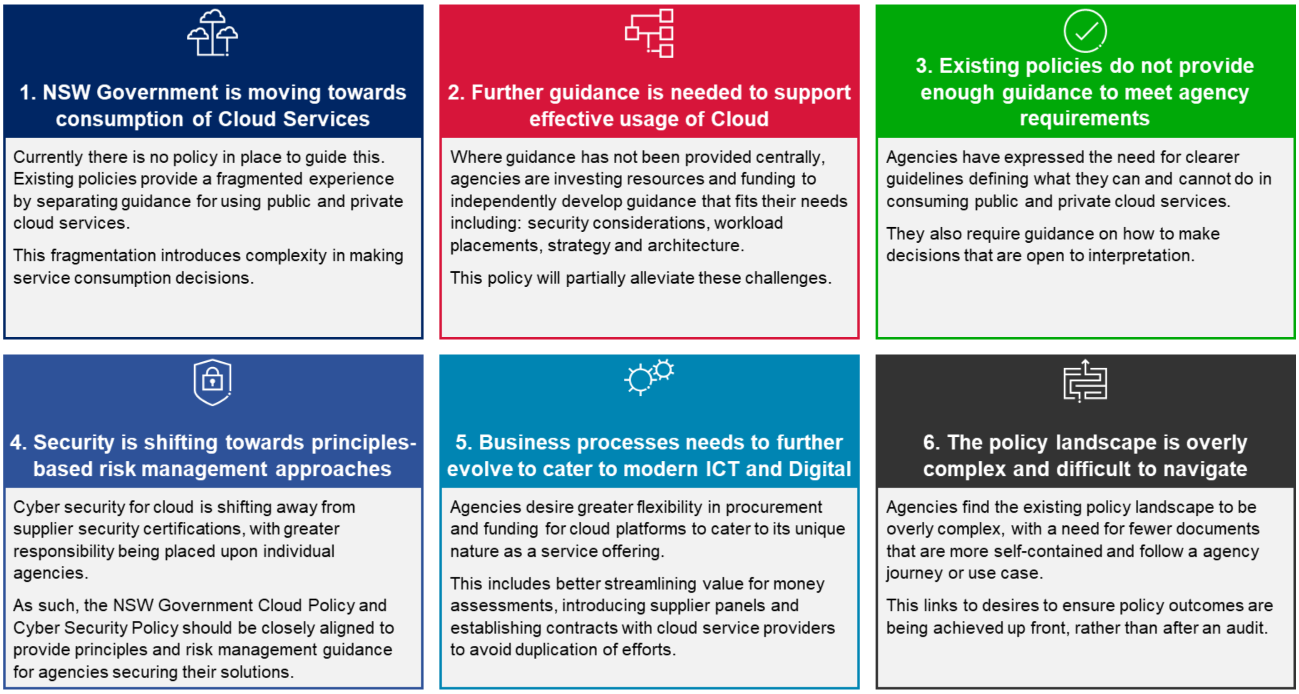
Stakeholder Perspectives

NSW Government agency stakeholders were engaged to understand common challenges and perspectives in using the existing policy landscape and to ensure the NSW Government Cloud Policy was relevant and fit for purpose.

Key findings from these NSW Government agency meetings were:

1. NSW Government is moving towards consumption of cloud, both public and Private
2. Further guidance is needed to influence the effective usage of cloud services
3. Existing policies do not provide enough guidance to meet NSW Government agency requirements
4. Cyber security is shifting towards more principles based, risk management approaches
5. Business processes needs to further evolve to cater to modern ICT and digital solutions
6. The existing policy landscape is overly complex and difficult to navigate.

These findings, detailed in the diagram below, have informed the development of the NSW Government Cloud Policy.



1. NSW Government is moving towards consumption of Cloud Services

Currently there is no policy in place to guide this. Existing policies provide a fragmented experience by separating guidance for using public and private cloud services.

This fragmentation introduces complexity in making service consumption decisions.

2. Further guidance is needed to support effective usage of Cloud

Where guidance has not been provided centrally, agencies are investing resources and funding to independently develop guidance that fits their needs including: security considerations, workload placements, strategy and architecture.

This policy will partially alleviate these challenges.

3. Existing policies do not provide enough guidance to meet agency requirements

Agencies have expressed the need for clearer guidelines defining what they can and cannot do in consuming public and private cloud services.

They also require guidance on how to make decisions that are open to interpretation.

4. Security is shifting towards principles-based risk management approaches

Cyber security for cloud is shifting away from supplier security certifications, with greater responsibility being placed upon individual agencies.

As such, the NSW Government Cloud Policy and Cyber Security Policy should be closely aligned to provide principles and risk management guidance for agencies securing their solutions.

5. Business processes needs to further evolve to cater to modern ICT and Digital

Agencies desire greater flexibility in procurement and funding for cloud platforms to cater to its unique nature as a service offering.

This includes better streamlining value for money assessments, introducing supplier panels and establishing contracts with cloud service providers to avoid duplication of efforts.

6. The policy landscape is overly complex and difficult to navigate

Agencies find the existing policy landscape to be overly complex, with a need for fewer documents that are more self-contained and follow a agency journey or use case.

This links to desires to ensure policy outcomes are being achieved up front, rather than after an audit.

Figure 3 - Themes from Stakeholder Meetings

6.2 Further Resources

For further information, please refer to the relevant resources listed below.

- buy.NSW
- Fact Sheet Supporting the Financial and Economic Analysis of Cloud Services and 'as-a-service' Solutions
- GIPAA Compliance Checklist for Agencies
- Government Information (Public Access) Act 2009 (GIPAA)
- Health Records and Information Privacy Act 2002 (HRIPA)
- ISO 31000 Risk management – Principles and guidelines
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27018 Information technology – Security techniques – Code of practice for protection of personally
- Identifiable information (PII) in public clouds acting as PII processors
- NSW Government Cyber Security Policy
- NSW Government as a Service ICT Sourcing Guide
- NSW Government Information Classification and Labelling Guidelines
- NSW Government Digital Information Security Policy
- NSW Government Digital Restart Fund
- NSW Government Guidelines for Economic Appraisal (TPP07-05)
- NSW Government ICT Investment Policy and Guidelines
- NSW Government Beyond Digital Strategy
- NSW Government Open Data Policy
- NSW Procurement Government Procurement Guidelines – Risk Management
- Internal Audit and Risk Management Policy for the NSW Public Sector (TPP09-05)
- OFS C2013-8 Data Centre Reform Strategy (archived)
- Privacy Act 1988 (Cth)
- Privacy and Personal Information Protection Act 1998 (PPIPA)
- Procure IT Framework (Version 3.2)
- Procurement Policy Framework (with Appendix B: Procurement practice checklist)
- State Records Act 1998
- State Records NSW Standard on Records Management
- Transition Guidelines: Managing Legacy Data and Information