POLICY UNDER REVIEW

FOR INFORMATION, CONTACT

ICTPOLICY@FINANCE.NSW.GOV.AU

This policy remains active. Due to website migration, resource links in this policy document have been disabled. Where appropriate, dates and version numbers have been referenced. To obtain copies, please contact ictpolicy@finance.nsw.gov.au.

NSW Government

Cloud Policy

April 2018

Version 2.1

Contact

Department of Finance, Services and Innovation
McKell Building
2-24 Rawson Place
SYDNEY NSW 2000

Contents

1. Introduction

In August 2013, the NSW Government published the *NSW Government Cloud Services Policy and Guidelines*. Since the publication of the policy, agencies have made significant progress in successfully transitioning to the cloud. Agencies have reported that the use of cloud-based services has led to more streamlined procurement, more effective pricing, agility and scalability, and greater flexibility in how they consume services. Cloud continues to facilitate transformational opportunities across government operations, enabling the delivery of citizen focused services anywhere, anytime and across platforms.

The NSW Government has put in place the policy framework, tools and infrastructure to enable the adoption of cloud-based services across government. This has included the publication of the *NSW ICT Investment Policy and Guidelines (February 2014),* reforms to the procurement framework, development of the ICT Services Catalogue, and the opening of two government data centres (GovDC) providing as a service solutions to agencies. Meanwhile, the market in cloud-based offerings has also matured substantially.

Key additions in version 2.0 of the policy are: more context, including framework pieces implemented since the original policy was released; inclusion of practical steps, to assist agencies with transitioning to the cloud (section 7); concise considerations for moving to the cloud (sections 8 and 9); cloud case studies showcasing examples of agencies achieving benefits in moving to the cloud (section 10); a table listing the types of services that NSW Government expects would be procured from the cloud (section 11); and an updated glossary (section 12).

2. Policy statement

NSW Government agencies will evaluate cloud-based services when undertaking all ICT procurements. The decision on the appropriate ICT delivery model will be based on an assessment of the business case, including the cost benefit analysis and achieving value for money over the life of the investment.

The positive experience of NSW agencies so far with the benefits of cloud services leads to the expectation that ICT procurements for commoditisable, non-core business solutions will be provided via cloud-based services – unless there is a specific consideration preventing this from happening. These services would ordinarily be procured from the ICT Services Catalogue or the GovDC Marketplace.

To assist agencies with their own transition to the cloud, to help inform the ICT investment process and the ICT Leadership Group of agency progress, principal departments should develop their own cloud transition strategies, which may form part of their existing ICT strategies. These should be submitted to the NSW ICT Leadership Group (via OFS) within six months of the publication of this policy. The table in Section 11 lists the types of systems that NSW Government expects would be procured from the cloud.

3. Purpose

This policy provides guidance for NSW Government agencies on approaching cloud procurements, and helps them determine which cloud delivery model is best suited to their business needs. This evaluation includes the business case, cost-benefit considerations, compliance, privacy and risk assessment. Agencies can also use the considerations outlined in this policy as guidance in reviewing existing cloud solutions.

4. Scope

This policy applies to all NSW Government Departments, Statutory Bodies and Shared Service Providers. It does not apply to State Owned Corporations, however, it is recommended for adoption.

This policy applies to the cloud-based variants of IaaS, PaaS, SaaS and BPaaS. It applies to public cloud, private cloud, and community cloud implementations as well as any hybrid of cloud solutions or cloud and non-cloud hybrid solutions.

5. Responsibility

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

6. Supporting mechanisms

Mechanisms have been established to support agencies as they move to a service orientation. When moving to cloud, agencies should consider whether the solution is fit for purpose, whether it achieves best value for money, and whether it provides adequate risk management.

Governance and strategic oversight is provided by the NSW Government ICT Board and ICT Leadership Group, with the ICT Advisory Panel contributing industry expertise.

ICT sourcing and procurement

The *Procurement Policy Framework* (July 2015, Version 4) provides the foundation for as a service procurements, emphasising:

- value for money
- market contestability
- innovation
- effective engagement
- fairness; and
- probity in government procurements.

The Procure IT framework version 3.1 is used by NSW Government buyers to purchase ICT goods and services. Cloud services can be procured using Module 10 As a Service and Module 11 Telecommunications as a Service.

Suppliers register to offer services to government through the ICT Services Scheme, an 'always open' prequalification arrangement designed to simplify processes for agencies and suppliers and improve opportunities for small and medium enterprises. Included in the supplier's registration is the commitment and understanding that services will be contracted and delivered under the terms and conditions of the NSW Government Procure IT Framework.

Agencies purchase services through the ICT Services Catalogue. The catalogue lists suppliers registered through the ICT Services Scheme and will help agencies find and procure ICT as a service. A number of as a service standards are produced by the NSW Government ICT Procurement and Technical Standards Working Group, a governance body under the ICT Leadership Group. The standards provide suppliers and government buyers with minimum government requirements for cloud-based services.

Examples of standards include: software asset management, end user computing, messaging and unified communications. The standards focus on as a service, and they help signal the government's strategic requirements and direction to vendors. Services which meet the standards are then endorsed by NSW

Government through the Offer Endorsement Process (OEP) and made available on the ICT Services Catalogue.

GovDC Marketplace

The GovDC Marketplace is a secure environment for the provision of as a service solutions that meet minimum NSW Government requirements. Agencies can acquire services through the ICT Services Catalogue, or by contacting the GovDC team at govdc@finance.nsw.gov.au. See *OFS C2013-8 Data Centre Reform Strategy* for additional policy guidance on moving to GovDC.

ICT investment

The *NSW ICT Strategy* is focused on driving more coordinated and efficient ICT investments which deliver better public services and achieve better value for money. The *NSW ICT Investment Policy and Guidelines (2014)* requires agencies to demonstrate alignment with the NSW ICT Investment Principles, including as a service sourcing, in strategic planning and investment decisions.

The whole of government approach to ICT investment as outlined in the *ICT Investment Policy and Guidelines (2014)* supports government to maximise opportunities for contemporary ICT investment, in line with the *NSW ICT Strategy*. Guidance is contained in the *As a Service ICT Sourcing Guide (November 2015)* and detailed guidance on developing business cases is available in the *ICT Investment Policy and Guidelines, Guidelines for Capital Business Cases (TPP08-05) and Gateway Review System (TC 10/13)*.

7. Practical steps

Experience with cloud solutions in NSW and internationally has revealed practical lessons that agencies can incorporate into their approaches to maximise the benefits of cloud and help address key considerations. Some of these may be reflected in an agency's cloud transition strategy.

Before transition:

- Define the desired business outcomes and appropriate use cases, and validate with internal and external stakeholders and peers as necessary. Ensure non-business critical elements are removed.
- Assess information requirements in terms of privacy, security, sensitivity, access and regulatory compliance.
- Start with non-critical systems with less information sensitivity in transitioning to the cloud.
- Understand the business and technological impacts of the transformation on processes, people and policies. Understand system and business process integration requirements.
- Invest effort in developing intellectual property that defines the business capabilities and processes that are being enabled with cloud solutions. Collaborate on and share this intellectual property with peers and industry as a way to achieve better solution designs.
- Be pragmatic, and balance risk and reward when choosing a solution.
- Align the application workload with business strategy.
- Consider how to leverage solutions from other jurisdictions, or building on already-established initiatives in other agencies.
- Use refresh points as triggers for evaluating cloud options.
- Apply leadership, collaborative approaches and innovation in strategic cloud procurements.
- Consider software asset management and rationalisation, together with applicable solutions available in the ICT Services Catalogue.

- Consider guidance on cloud, including the *As a Service ICT Sourcing Guide (2015)*, discuss plans with early adopter peers, and contact ictpolicy@finance.nsw.gov.au with outstanding queries.

Cloud contracting and management:

- Depending on the level of experience of the solution provider, consider provider management requirements, performance visibility, troubleshooting processes and arrangements for access, if necessary.
- Ensure transparency in supply contracts and in each part of the supply chain, including alignment with agency risk management policies and processes.
- Monitor cloud key performance indicators, including availability and reliability.
- Ensure appropriate assurance and reporting by providers and monitoring by agencies in relation to security controls, business continuity and disaster recovery.
- Plan for scenarios where the service may be interrupted, terminated, or the agency wishes to transition out of the service, to ensure business continuity.

8. Considerations

When moving to cloud, agencies should consider:

- **Cost-benefit** analysis of moving to a specific cloud solution. This covers value for money, fit for purpose, a clearly defined business case (with benefits realisation reporting), the total cost of ownership (TCO), asset impact, organisational impact and the technical environment. Refer to the *Fact Sheet Supporting the Financial and Economic Analysis of Cloud Services and 'as-a-service' Solutions (March 2015)* for further guidance.
- **Change management** – transitioning in and out of the service, with reference to the *Information Management Framework – Change Management Guidance*. Consider software licensing issues that could arise.
- **Technical and network requirements**, with considerations such as: enterprise architecture, bandwidth, response time, capacity, priority, availability, firewalling, automation, virtualisation, compatibility, interoperability and configuration. Ensure vendor lock-in is avoided.
- **Information and records management**, including exactly where the information will be stored geographically (particularly if it includes sensitive or personal information), access, governance, custodianship, classification and labelling, data and intellectual property ownership.
- **Risk management** as with any investment undertake a risk assessment.
- **Security** and whether the cloud service provider is compliant with the *Digital Information Security Policy* and with *ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*
- **Privacy** and whether the cloud service provider meets NSW information privacy laws and any other applicable privacy laws.
- **Agency skills, capabilities and workforce management**, ensuring the agency has sufficient workforce capability to move from on-premises technology management skills to virtual service governance with contract management and solution oversight.

Information and records management

Refer to the *NSW Information Management Framework* for an overview of information governance in

NSW. The *State Records Act 1998* is the primary instrument regarding the creation, management, protection and on-going accessibility of records of public offices in NSW. State records may be stored outside of NSW via cloud services – see State Records guidance *Using Cloud Computing Services (revised September 2015)* and *Storage of State records with service providers outside of NSW (revised January 2015)* for more details.

The provisions governing storing records outside of NSW are contained in section 21(2)(c) of the *State Records Act 1998* and General Authority 35 (GA35). Sending records for storage with, or maintenance by, service providers based outside NSW is permitted – provided that an appropriate risk assessment has been done, and records are managed in accordance with all the requirements applicable to State records.

Care must be taken not to take or send records out of the State in contravention of any legal responsibilities or business interests the agency may have. Further information is provided *Storage of State records with service providers outside of NSW.*

Agencies must ensure that records and data created, stored or managed in the cloud remain accessible and retrievable in order to meet regulatory requirements for information access, e.g. under *Government Information (Public Access) Act 2009* (GIPAA), *Privacy and Personal Information Protection Act 1998* (PPIPA) and *Health Records and Privacy Information Act 2002* (HRIPA). GIPAA gives members of the public an enforceable right to access government information. PPIPA and HRIPA also give individuals the right to access their personal and health information held by public sector agencies. The broad issues to be considered include:

- is agency access to data guaranteed?
- can agencies provide relevant information to third parties (such as to individuals to whom the data relates or regulators monitoring compliance with legislative requirements)?
- can the agency audit data access?
- how will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?

State Records provides further guidance in the *Standard on records management (revised October 2017).*

Risk management

Agencies must undertake comprehensive risk assessments in relation to network access, storage and maintenance of public sector information and records held by cloud providers. As agencies evaluate ICT delivery options, risk profile assessments will be required for each option. A full understanding of the risks and opportunities associated with cloud-based solutions is critical, both from an end-user and delivery capability perspective. Evaluation of cloud options will address all identified risks and take account of:

- *Digital Information Security Policy (April 2015, Version 2.0)*
- *Internal Audit and Risk Management Policy for the NSW Public Sector (TPP09-05)*
- *ISO 31000 Risk management – Principles and guidelines*
- *ISO/IEC 27018.*

Depending upon the service type, business need and delivery model adopted, an understanding and mitigation of risks will be required. This includes, but is not limited to: data location and retrieval, legal and regulatory risk, information governance and management, business continuity, security, privacy and licensing. Business continuity and disaster recovery plans must be well documented and

tested. Existing software licensing models may not seamlessly translate to a cloud deployment solution.

Under GA35, where records are being transferred outside of NSW for storage with or maintenance by service providers based outside NSW, public offices must:

- assess and address the risks involved in taking and sending records out of the State for storage with or maintenance by service providers based outside of NSW
- ensure the service providers facilities and services conform to requirements in standards issued by State Records
- ensure contractual arrangements and controls are in place for the safe custody and proper preservation of records
- ensure that the ownership of the records remains with the public office
- monitor the arrangement to ensure the service provider is meeting relevant requirements.

Security

The *Digital Information Security Policy* establishes digital information security requirements for the NSW public sector, including the requirement to have an Information Security Management System (ISMS) that demonstrates compliance with a minimum set of controls, and requirements relating to certification, attestation and the nomination of Senior Responsible Officers to the NSW Digital Information Security Community of Practice.

Agencies must ensure that any cloud-based service complies with the agency's ISMS and the requirements of the *Digital Information Security Policy*. Relevant international standards include *ISO/IEC 27001 Information technology – Security techniques – Information security management systems* and *ISO/IEC 27018*.

Privacy

The collection, storage, access, use and disclosure of personal information is governed by PPIPA and HRIPA. Where the use of cloud computing requires the transmission or storage of personal information, including health information, agencies must ensure that their arrangements comply with relevant privacy and disclosure requirements.

An agency must not do anything, or engage in any practice, that contravenes an Information Protection Principle or a Health Privacy Principle applying to the agency. Particular areas of cloud services which may impact data privacy include:

- disclosure of personal information to a cloud service provider
- data security and safeguards against misuse or loss, unauthorised access, use, or alteration
- ensuring ongoing accessibility for the agency and data subject
- legislative environment and governing data laws in the location where data is stored
- determining who has control of data at the end of a contract
- authorised data retention and disposal.

If an agency shares with or transfers personal information to a contracted cloud service provider and the cloud service provider simply holds the data and acts according to the instructions of the agency, then

disclosure will not be considered to have occurred. If the cloud service provider uses the data provided for its own purposes, this may be unauthorised access, use, modification or disclosure.

Agencies must ensure that contractual arrangements with a cloud service provider explicitly address this, and take such security safeguards as are reasonable in the circumstances to prevent unauthorised access or use. These arrangements will need to take into account circumstances that may include where one or more functions of an agency are outsourced to a provider, or where a cloud service provider is asked to perform some action on the personal information which they had previously only been storing.

An international standard, *ISO/IEC 27018*, was issued in mid-2014 on security and privacy for cloud providers. This standard establishes objectives, controls and guidelines for implementing measures to protect personal information for cloud vendors that use a public cloud computing environment.

Agencies should refer to their Privacy Management Plan and the IPC Checklist to help identify privacy issues relating to proposed cloud services solutions.

Agency skills, capabilities and workforce management

The *NSW ICT Strategy* identified people as a key enabler of improved service delivery and better value ICT investment, and outlined actions that will help to develop ICT skills and capabilities across the NSW public sector.

The migration to a new system, regardless of the delivery model, will require assessment of the agency's workforce capability. Ensuring agencies have skills and capabilities to move to the cloud necessarily involves a shift to a greater emphasis on as a service skills, and a growing need for contract negotiation, business analysis, portfolio/program management, vendor/contract management, managing service level agreements (SLAs) and service design skills.

There may also be implications for agency skills and capabilities requirements through the implementation of cloud services, for example, where commercial off-the-shelf solutions are used and business processes need to be modified.

The NSW Public Sector Capability Framework and the Skills Framework for the Information Age (SFIA) together provide the common foundation tool to support the full range of workforce management strategies and development activities across NSW Government. Undertaking existing and future functional and capability analysis will include a broad assessment of the resource level needed to deliver each function as well as workforce capabilities and status.

9. Contract terms

It is recommended agencies develop a sound understanding of the fundamental issues to be addressed in cloud services contracts. Procure IT provides a mandatory suite of standard documents, terms and conditions for ICT contracting for NSW Government agencies. Modules with standard contract terms and conditions for as-a-service ICT models are available, in particular Module 10 As a Service.

Agencies will undertake risk assessment, due diligence and privacy impact assessments, with specific issues being identified through the compliance and risk assessment processes, according to the type of service and delivery model that best meets the agency requirements and risk profile. Appropriate contract terms ensure an agency retains sufficient control over its data to meet regulatory obligations, and they ensure a provider is legally bound to meet the agency's instructions.

Custody and ownership

While evaluating or negotiating cloud services, public sector agencies must ensure that NSW Government retains ownership of its information assets. Contractual provisions should:

- Explicitly state that the agency is the owner of all rights, title and interest in the data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer or destruction of the data)
- Identify the actual geographic locations where data storage and processing will occur
- Confirm the jurisdiction which governs the operation of the contract, and application of privacy, confidentiality, access and information management laws
- Confine data storage and processing to specified locations where the regulatory framework and technical infrastructure allow the public agency to maintain adequate control over the data.

Security, privacy and access

It is essential that any engagement with a cloud service provider guarantees the security of data and provides for notification of breaches. Legislation requires agencies to maintain control over the accessibility of their data, and cloud service providers should be able to demonstrate compliance with PPIPA, HRIPA, GIPAA, the *State Records Act 1998*, and any other applicable laws (e.g. the *Privacy Act 1988 (Cth)*).

Contractual provisions to consider:

- Specific security standards with which the provider must demonstrate compliance, including a warranty in relation to security, related storage and access obligations, and SLAs that include cost and operating requirements of providing service continuation in business critical and non-business critical services when disruptions arise.
- Prescribe the security provisions the service provider must implement, consistent with the *Digital Information Security Policy* (and where required, certified compliance with *ISO/IEC 27001*), and *ISO/IEC 27018.*
- Prohibit any unauthorised access, use or alteration of the data. Document the technical mechanisms and procedures in place to support this restriction (e.g. agency control of user credentials for authentication, data encryption, information dispersal, data separation and segregation). Ensure that the contract prevents unauthorised access or use by the service provider or sub-contractor, including any 'third party use' of data.
- The computing processes by which the cloud service provider secures its information and the encryption between agencies and any overseas cloud storage location should be investigated and guaranteed by contractual terms.
- Contractual arrangements should allow agencies to receive data breach notifications.
- The security obligations imposed by the agreement on the cloud service provider should include the terms of the provider's ISMS.
- Specify that government information is subject to GIPAA, which facilitates information sharing and proactive disclosure of information, along with the *NSW Open Data Policy*. GIPAA requests can also be for personal information. More guidance is available in the *GIPAA Compliance Checklist for*

Agencies.

- Specify that any personal information contained in the data is subject to PPIPA, HRIPA and any other applicable privacy laws. This would include that any person or body providing data services (relating to the collection, processing, disclosure or use of personal information) for, or on behalf of, a public sector agency must abide by the Information Protection Principles and the Health Privacy Principles.
- State that the agency retains an immediate and ongoing right of access to all agency data held by the cloud service provider. The service provider should provide the links to connect to its service.
- Include provisions allowing auditing of the data or the service in line with policy and legislative requirements.

Business continuity, data disposal and transition out

Agencies must be able to guarantee the accuracy, integrity and reliability of data to ensure the ongoing availability of the data and maintain control over its retention or disposal. Agencies should also have a contingency plan to migrate data securely to another solution or provider or agency. Contractual provisions to consider:

- Document the technical mechanisms and procedures that prevent data loss (for example: contractor/agency responsibilities and routines for backup, failover or redundancy).
- Provisions for continuity of accessibility, usability and preservation of all agency data regardless of any migration of data to other formats during the contract. Terms should provide for appropriate testing to ensure data integrity prior to any migration.
- Specify provisions and procedures for backup, restoration of services and disaster recovery.
- Upon transfer of data, ensure technological parity with other service providers is guaranteed.
- Contractual arrangements should guarantee the preservation of data and provide for routine monitoring of data in order to identify formats that are at risk of obsolescence.
- Contractual arrangements should include provisions relating to migration of data to new formats when appropriate and the provision of proper documentation about migration activities to the agency.
- Provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover.
- At the termination of the agreement with a cloud service provider, specify what will happen to the data (e.g. transfer to a new provider, returned to the agency, permanently deleted).
- Specify remedies for service provider mistakes or breaches.
- Ensure that the client (government agency) does not have to first prove that the root cause of an issue is not on the client side *before* the issue will be addressed by the provider, to facilitate timely resolution of any issues that may emerge.
- Identify any penalty provisions imposed by the service provider (e.g. suspension of agency access to data for non-payment).
- Define contract provisions relating to migration of data on termination of the contract.

- Precise terms for the disposal of specific data (a) during the term, at the request of the agency; and (b) at the end of the term, including a warranty in relation to technological parity/obsolescence.
- Limit any suspension and termination rights available to the cloud service provider.
- Subscription levels should be scalable up and down according to demand.
- Reporting and audit rights of the client and vendor should be contractually explicit.

10.Case studies

NSW Government agencies are taking advantage of cloud sourcing models, with benefits in cost, consumption-based pricing, agility, scalability, reliability, innovation, resilience, productivity, standardisation and in-built upgrades. Common cloud service models include SaaS, PaaS, IaaS, BPaas and common deployment models include private, public, hybrid and community clouds.

Through experiences transitioning to the cloud, NSW agencies have improved their practices and lessons are being shared across government.

ServiceFirst implementation of unified communications

ServiceFirst recently undertook a strategic review to enhance unified communications (UC) capabilities for client agencies, including considering the cost to support disparate legacy PABX and fixed voice implementations. With the migration to Microsoft productivity technologies predominantly complete, there is now a blend of UC (Lync) and PABX environments. As UC technologies such as Lync advanced to providing external phone call capabilities, the overlap of the old and new technologies was increasing.

The roadmap is to leverage the Lync UC solution as the enterprise voice platform and shift away from high cost legacy based PABX fixed voice technologies. To do this ServiceFirst partnered with a vendor to deliver UC as a service on a pay per user per annum basis. The service is hosted by GovDC, which is designed for multi-tenant capability which will enable the service to be provided to non-ServiceFirst clients in future.

Mobile users will be able to roam with full UC capability (instant messaging, collaboration, desktop sharing, voice and video). This solution will soon be integrated into the Cisco (meeting room) video conferencing service to allow Lync users to participate from wherever they are connected to the network (office, home, airport etc.). The service provides many benefits, including rapidly configurable solutions, anywhere availability of government employees, number portability, and scalability of services. There is also a cost reduction in phone charges, as all internal calls between ServiceFirst clients will traverse our WAN at zero cost, as opposed to the public network at the cost of a local or national call.

Fire and Rescue implementation of Microsoft Office 365

Fire and Rescue moved its email system to Microsoft Office 365 in 2013. In 2015, the agency is now enabling the full feature set of Office 365 and making it the centrepiece of its mobility strategy. By leveraging this cloud email and cloud drive (OneDrive) solution, the agency can retire its internal shared drives. In combination with providing a web interface to its business applications, the agency can begin to access email, shared drives and business applications on unmanaged devices via a web browser using the internet. This capability brings with it substantial flexibility, simplicity, improved access to systems and information, and substantial savings.

In early 2014, Fire and Rescue NSW's corporate infrastructure (servers and storage) were at end of life. The Infrastructure group was also having difficulty providing 24 hour support with a relatively small team. The

agency understood that PaaS enabled it to leverage the scale, skills and support capability of external service providers for whom these services were core business.

After a competitive tender, the agency became the first agency to move to PaaS through the NSW GovDC data centres. The result was a significant improvement in performance, flexibility and support. With the scalability of the solution, add-on services can be procured, which further increases the value provided.

Trade and Investment implementation of ERP as a service

Trade and Investment has implemented enterprise resource planning (ERP) as a service, leading to greater efficiency in its business and management processes. The agency was maintaining disparate systems, and there was not a clear single view of the business and its operations.

To consolidate the numerous independent finance, procurement, projects, payroll and HR systems, the agency chose to move to a SAP cloud ERP service. The service enables the agency to manage finance, procurement and sourcing functionality from servers based in Germany. Bringing all member agencies and institutions into a single ERP system has resulted in significant savings for the agency, with consolidated systems, controls, processes and data. A high level executive team was responsible for project implementation from start to finish, with no intermediary, and the project was considered a major organisational priority.

The focus stayed on adopting the solution with minimal customisation; this required the business to be disciplined and to change its practices to enable the adoption of a standard contract with minimal change requests.

Family and Community Services implementation of a cloud-enabled email service

Family and Community Services provides a cloud-enabled email service for approximately 27,000 mailboxes across NSW Government agencies. The agency migrated mailboxes from an ageing platform to a fully featured environment in a privately hosted data centre.

The solution is based on a pay-as-you-go model for messaging to align with government strategy to consume ICT services as they are needed. The solution is having a significant community impact, with case workers across NSW able to access email and calendars on their mobile devices. This means frontline workers can spend more time helping citizens in need of their services. The provider supports ‘evergreen’ ongoing upgrades, so the agency always has access to the latest version of the messaging platform.

The migration process has shown the need to introduce both sourcing and project management capability early in the project to manage cloud migration and service integration, by comparison with a traditionally designed and built project. Additionally, reducing mailbox sizes or data migration requirements aid in the speed of the migration effort and reduce co-existence issues.

11.Services procured from the cloud

Services that can be commoditised, or are ancillary to core agency activity, can be procured from the cloud, as these have the lowest managed risk and highest potential benefit from the transition to the cloud. Business processes in these applications are increasingly uniform and standardised across whole of government, increasing quality and helping to drive down operating costs.

The following table lists services that NSW Government expects would be procured from the cloud.

Software development, testing and preproduction
Technology operations
Quality assurance
Workforce and Human Capital Management (HCM)
Timesheeting
Document management
Enterprise Resource Planning (ERP)
Standardised business process management (BPM)
Procurement
Transactional services
Training, eLearning
Customer Relationship Management (CRM)
Messaging, collaboration and unified communications
Service desk management
Case management
Software Asset Management (SAM)
Print services

Other types of services that agencies should consider procuring from the cloud include end user computing, compute, storage, data warehousing, business intelligence and analytics services.

12.Glossary

(Based on US National Institute of Standards and Technology (NIST) and Australian Signals Directorate (ASD) definitions)

As a service (aaS)	As a service – Refers to *how* the solution is provided. "As a service" usually refers to services that are delivered via the cloud rather than locally or on-site, although this is not always the case. As a service solution components are usually funded from an operating expenditure budget unlike capital intensive ICT infrastructure and equipment.
BPaaS	Business process as a service – Delivery of business process outsourcing (BPO) services that are sourced from the cloud, accessed via internet technologies, usually automated, and constructed for multi-tenancy. BPaaS drives standardisation of business processes across NSW Government as normal commoditised activities move to best practice, e.g. payroll.

Cloud-based services	On-demand delivery of ICT services over a network, commonly over the internet, from a shared pool of computing resources. "Cloud" usually refers to *where* the solution is provided. Key characteristics of cloud-based services are: • On demand self-service • Broad network access • Resource pooling • Rapid elasticity • Measured service with unit based pricing
Community cloud	Exclusively shared by a number of organisations with common objectives, and it may be on or off premises. An example may be the sharing of cloud infrastructure among a number of agencies of the same government.
Hybrid cloud	A cloud deployment using at least two different cloud deployment models. An example is using resources from a public cloud for displaying non-sensitive data, which interacts with sensitive data stored or processed in a private cloud.
IaaS	Infrastructure as a service – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources. The consumer is able to deploy and run arbitrary software, which can include operating systems and applications. Computing power, networking and storage is provided.
PaaS	Platform as a service – Where applications can be developed and executed. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
Private cloud	Provided solely for the use of one organisation and managed by that organisation or by a third party, provided at the organisation's premises or off-site.
Public cloud	The cloud infrastructure is shared via the internet with many other organisations and members of the public.
Refresh point	For example, when business ICT systems are due for replacement, or in the case of planned system implementation/upgrades.
SaaS	Software as a service – The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. Full application functionality is delivered.

13.Sources

Digital+ 2014-15 ICT Strategy Update
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")
Guidelines for Capital Business Cases (TPP08-05)
Health Records and Information Privacy Act 2002 ("HRIPA")

Information Management Framework – Change Management Guidance
Information Management: A Common Approach
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
NIST Definition of Cloud Computing 800-145
NSW Government as a Service ICT Sourcing Guide
NSW Government Information Classification and Labelling Guidelines
NSW Government Digital Information Security Policy
NSW Government Guidelines for Economic Appraisal (TPP07-05)
NSW Government ICT Investment Policy and Guidelines
NSW Government ICT 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
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

14.Document control

Date	Version No.	Description	Author
August 2013	1.0	Final	Office of Finance and Services
June 2015	2.0	Final	Office of Finance and Services
April 2018	2.1	Updated contact information and amended hyperlinks	Department of Finance, Services and Innovation

Contact: ICT Policy, ICT & Digital Government, Department of Finance, Services and Innovation
Email: ictpolicy@finance.nsw.gov.au

This policy will be reviewed in twenty-four months from the issue date, or earlier in response to post-implementation feedback from departments.