NSW Government

Data Centre & Cloud Readiness
Assessment Services Standard

v1.0

June 2015

ICT Services
Office of Finance & Services
McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
standards@finance.nsw.gov.au
## CONTENTS

1. **CONTEXT**  
   1.1. Background  
   1.2. Purpose  
   1.3. Scope and application  
   1.4. Policy  
   1.5. The ICT Services Catalogue  

2. **KEY PRINCIPLES**  

3. **REQUIREMENTS**  
   3.1. Data centre and cloud readiness summary  
   3.2. Elements  

**DOCUMENT CONTROL**  

**APPENDIX A – GLOSSARY**  

**APPENDIX B – REFERENCES**  

**APPENDIX C – STANDARDS**  
   Developing standards  
   Management and implementation  

**APPENDIX D – NABERS ENERGY RATINGS**
1. CONTEXT

1.1. Background

This is a technical standard developed through the NSW ICT Procurement and Technical Standards Working Group. This standard defines minimum government requirements for professional services that assist agencies with moving to data centres and the cloud.

By defining the necessary and common elements across agencies this standard provides an opportunity to leverage the buying power of Government as a whole and reduce inefficiencies by increasing interoperability.

1.2. Purpose

The purpose of this standard is to assist NSW Government agencies with obtaining professional services to help them develop, procure and implement data centre and cloud readiness solutions or tools, as well as take full advantage of the benefits of these solutions or tools.

This standard details the issues that need to be considered so each agency can identify the available options that best suit their business requirements, helping agencies achieve value for money through cost savings and improved flexibility of service offerings, and ensuring they can take full advantage of the benefits of federated and remote identity management solutions.

1.3. Scope and application

This standard covers the provision of professional services to assist agencies in the transition of data centre facilities and/or services to the Government Data Centres (GovDC), or to ensure agencies are ready to obtain services from the cloud. For the purpose of this standard the following meanings apply:

- **Data centre**, meaning all back-end IT systems (including mainframes, servers and databases) used for remote storage, management, processing and/or distribution of data that an agency intends to retain (either internally managed or through external managed arrangements), and
- **Cloud readiness**, meaning all elements of a supplier’s offering relating to cloud transition, migration and cloud readiness assessment.

This standard does not exhaustively cover all agency specific considerations. Agencies may need to assess any specific requirements they have in addition to those detailed in this standard.

This standard applies to all NSW Government departments, statutory bodies and shared service providers. It does not apply to state owned corporations, but is recommended for their adoption.

1.4. Policy

The **NSW Government ICT Strategy** sets out the Government’s plan to build capability across the NSW public sector to deliver better, more customer-focused services that are available anywhere, anytime, and derive better value from the Government’s annual investment in ICT.

Developing whole of NSW Government ICT technical standards is a key initiative of the **NSW Government ICT Strategy**, driven by the ICT Procurement and Technical Standards Working Group. These standards leverage principles defined in the **NSW Government ICT Strategy**, the **NSW Government Cloud Services Policy and Guidelines**, the **Data Centre Reform Strategy**, and they support the NSW ICT Services Catalogue. In procuring ICT services agencies should also have regard to the NSW Government ICT investment principles, set out in **NSW Government ICT Investment Policy and Guidelines**.
The standards set out service definitions as minimum requirements that vendors must meet to be able to offer their services through the NSW Service Catalogue. This helps achieve consistency across service offerings, emphasising a move to as-a-service sourcing strategies in line with the NSW Government ICT Strategy, and it signals government procurement priorities to industry.

This standard should be applied along with existing standards, policies and guidance that make up the NSW Information Management Framework, as set out in the Information Management: A Common Approach, and including the NSW Digital Information Security Policy. In addition, solutions should assist agencies in their alignment with the NSW Government Enterprise Architecture Strategy.

NSW Government agencies must carefully consider their obligations to manage government data and information. Contract arrangements and business processes should address requirements for data security, privacy, access, storage, management, retention and disposal. ICT systems and services should support data exchange, portability and interoperability.

More information on the development of standards for the ICT Services Catalogue is at Appendix C – Standards.

1.5. The ICT Services Catalogue

The ICT Services Catalogue provides suppliers with a showcase for their products and services, and an opportunity to outline how their offerings meet or exceed standard government requirements.

The standards, together with supplier service offerings in the ICT Services Catalogue, help to reduce red tape and duplication of effort by allowing suppliers to submit service details once. The offerings are then available to all potential buyers, simplifying procurement processes for government agencies.

Implementing this category management approach is embedding common approaches, technologies and systems to maintain currency, improve interoperability and provide better value ICT investment across Government.

2. KEY PRINCIPLES

The following principles guide the development and implementation of this standard.

- **Prioritise low risk, low impact as a service implementations**: Many agencies will find that a useful approach is to start the transition to as-a-service sourcing models with implementations that are low risk and low impact. Low risk, low impact and high agility systems may be moved with minimal disruption. Agencies will be able to gain experience from these transitions, which can be applied to future moves, more complex implementations.

- **Change management planning**: Should include people, processes and organisational change. It should also include planning to achieve cultural acceptance of moving to as a service.

- **Facilitating as a service**: Specification of data centre and cloud environments will support agencies in moving to as a service sourcing models.

- **Interoperability**: Meeting this standard should help agencies achieve application and hardware interoperability, ensuring that agency environments enable appropriate information sharing across devices and applications.

- **Mobile and flexible**: The end user environment should support modern office work practices, including flexible working, activity based working and hot desking.
• **Vendor / operating environment agnostic:** Determining environments should be vendor and operating system agnostic. Devices such as laptops, notebooks, thin-clients etc. should be able to connect to, and access the network. The network must also be fully compatible with widely used operating environments.

3. **REQUIREMENTS**

3.1. **Data centre and cloud readiness summary**

This section provides a more detailed description of the data centre and cloud readiness services recommended business and technical requirements for NSW Government. It provides a consistent approach for all NSW Government agencies regardless of their size.
**Use Case / Scenarios – Data centre and cloud readiness**

‘Use cases’ that are anticipated in agencies are included in the table below.

The corresponding requirement sections of this standard are ticked in the columns.

<table>
<thead>
<tr>
<th>Use Case / Scenario</th>
<th>Data centre and cloud readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data centre</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud / As a service</td>
<td>✓</td>
</tr>
</tbody>
</table>
3.2. Elements

The elements outlined below cover both data centre and cloud readiness assessment requirements. Data centre and potential suppliers of data centre and cloud readiness professional services need to ensure they have the demonstrated capability to assist agencies in their moves to either (or both) NSW Government data centres and cloud (as a service) offerings.

By 30 August 2017, all data centre facilities must reside within the NSW Government Data Centre (GovDC) environment. For details of GovDC policy requirements see DFS C2013-8 Data Centre Reform Strategy.

The below elements align with the NSW Government as a Service ICT Sourcing Guide. Agencies and potential suppliers should consider that guide for a fuller understanding of the requirements of this standard.

DATA CENTRE

Data Centre Policy

Agencies must adhere to the following policy requirements:

1. For any data centre facility encompassing a physical environment, plant or real estate owned or leased by the agency, the contents must move to the new GovDC data centres by 30 August 2017 and the legacy facility shut (or lease terminated) and made good.

2. When procuring cloud services “Infrastructure as a Service”, “Platform as a Service”, or outsourcing existing management of ICT, agencies should request from suppliers as one of the tendered options, use of the GovDC data centres as the location of the services provided by that supplier. This includes web hosting.

3. In relation to “Software as a Service” arrangements, agencies should procure cloud based services in a manner consistent with broader ICT policy. Agencies should consider security and performance benefits of procuring these cloud based services from suppliers ‘on-site’ within the data centres, or through a secure gateway from within the data centres.

See Appendix D – Nabers Energy Ratings for details on data centre energy requirements.

Business (GovDC) Requirements

Provision of services that assist agencies develop core business requirements of the future service and establish parameters and key performance requirements. Elements will also include:

- Assessment of the agency technical environment to ensure it is ready to move to one or both GovDC facilities

- Ensure GovDC services align with the agency’s broader plans, systems and forecasted requirements, and

- Agency skill implications of moving to GovDC services.

NSW Government Data Centre

All relevant services for the solution to be provisioned from one or both NSW Government Data Centres (GovDC). Depending on the service offering and agency requirements, it may be possible to ‘burst’ some elements of services to other locations subject to agreement with OFS and the commissioning agency.

Burst hosting facility must be deemed ‘compliant’. If the ‘burst’ data centre facilities change to a location that is deemed unacceptable either to NSW Government or to the agency, the agency may need to re-examine the ‘burst’ service or the full service.
CLOUD / AS A SERVICE

Business (Cloud) Requirements

Provision of services that assist agencies develop core business requirements of the future service and establish parameters and key performance requirements. Elements will also include:

- Assessment of agency technical environment to ensure it is cloud ready
- Ensure cloud services align with the agency’s broader plans, systems and forecasted requirements
- Agency skill implications of moving to cloud services.
- The type of as a service being considered and its appropriateness to the agency’s business needs

Cloud Compliant Hosting Facility

All relevant cloud services for the solution are to be provisioned from a compliant hosting facility. Compliant hosting is defined as having the following attributes and/or capabilities:

- The location of the hosting facility must be identified either by name and/or location (city and country) in any response
- The hosting location cannot be changed without first informing the agency concerned
- The service provider undertakes, maintains and provides access to SSAE 16 Service Organization Control (SOC) Type II reports (or equivalent) for the services and facilities in scope for the engagement
- The hosting facility must comply with minimum Tier 3, as defined by the Uptime Institute, ANSI TIA-942, or an equivalent industry standard.
- The hosting facility must be certified against ISO 27001; compliance with the following international standards is desirable:
  - ISO 9001
  - ISO 27002
  - ISO 20000-1:2011
  - ISO 14001
- Other desirable certifications may include, but are not limited to:
  - PCI-DSS v3.0 or later
  - Australian Signals Directorate
  - ASIO-T4
  - Uptime Institute
  - CSA

Also consider contractual obligations relating to the service provider allowing security assessments and treatment of outcomes as agreed with the client.

If the hosting facilities changes to a location that is deemed unacceptable either to NSW Government or to the agency and/or loses attributes and/or capabilities identified above, the agency may need to consider termination of services.
GENERAL REQUIREMENTS

Information and Project Risk Assessment
Undertake information risk and project risk assessments sufficient that the agency can be assured all reasonable validations have been undertaken to ensure information contained in systems to be provided as a service is appropriately classified and labelled, and risk mitigation has been appropriately considered.

Knowledge of NSW Government Procurement Requirements
Suppliers of services must possess appropriate and current knowledge of NSW Government procurement requirements as a minimum relating to cloud service provisions. Wider knowledge should be considered an advantage.

Cost Benefit Analysis
Provision of cost benefit analysis services taking into account both the short and long term costs and benefits of moving to GovDC and/or consuming cloud based as a service offerings.

Information and Security Management
Suppliers of services must be able demonstrate current knowledge of NSW Government information management and information security requirements and be able to assist agencies in ensuring potential cloud and/or data centre service providers are compliant.

All NSW Government departments, statutory bodies and shared service providers must adhere to the NSW Government Digital Information Security Policy.

Contract Management
Service providers must be able to demonstrate understanding of current NSW Government contract management requirements together with current knowledge of transition in and transition out requirements for third party service providers.

Evaluation
Service providers must be able to demonstrate current knowledge of NSW Government evaluation process and practices to ensure agency compliance.

Service Level Management
Agencies will retain ultimate responsibility for service level management in any solutions engagement, which would ordinarily be covered by a service level agreement (SLA). Agencies, service-brokers and solution providers need to agree all SLA reporting and other related activities as part of any transition-in process.

Multi-service Broker Provision
Any solution provider must work within the confines of a multi-service provider environment where either the agency or nominated provider will perform broker service provision. This will be defined as one provider being made accountable for the provision of all associated services, whether these are provided by the provider itself, or other third-party providers.
DOCUMENT CONTROL

Document history

Status: Final
Version: 1.0
Approved by: Procurement and Technical Standards Working Group
Approved on: 4 June 2015
Issued by: NSW Office of Finance & Services
Contact: ICT Services, Service Innovation and Strategy Division, Office of Finance and Services
Email: standards@finance.nsw.gov.au
Telephone: (02) 9372 7445

Review

This standard will be reviewed in 12 months. It may be reviewed earlier in response to post-implementation feedback from agencies.
### APPENDIX A – GLOSSARY

This standard aligns with the definitions provided in the *NSW Government Cloud Services Policy and Guidelines*:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>As a service (aaS)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>BPaaS</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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. |
| **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. |
APPENDIX B – REFERENCES

Agencies should have regard to the following statutes, NSW Government policies and standards:

- ANSI TIA-942 – Telecommunications Infrastructure Standard for Data Centres
- AS/NZS ISO 31000 Risk management – Principles and guidelines
- Data Center Site Infrastructure Tier Standard: Topology, Uptime Institute
- DFS C2013-8 Data Centre Reform Strategy
- Electronic Transactions Act 2000
- Government Information (Information Commissioner) Act 2009
- Government Information (Public Access) Act 2009
- Health Records and Information Privacy Act 2002
- M2012-15 Digital Information Security Policy
- NSW Government as a Service ICT Sourcing Guide
- NSW Government Cloud Services Policy and Guidelines
- NSW Government Digital Information Security Policy
- NSW Government Enterprise Architecture Strategy
- NSW Government ICT Strategy NSW Government ICT Technical Standards – Mobility Standard
- NSW Government Information Classification and Labelling Guidelines
- NSW Government Open Data Policy
- Privacy and Personal Information Protection Act 1998
- Public Finance and Audit Act 1983
- Public Interest Disclosures Act 1994
- NSW Procurement: Small and Medium Enterprises Policy Framework
- State Records Act 1998
- Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization
- TPP 09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector
APPENDIX C – STANDARDS

Developing standards

Development of a standard begins with identifying the need for a new standard, which is followed by the development of the standard in consultation with the industry and experts groups, including the Australian Information Industry Association (AIIA).

The following diagram outlines the process.

The ICT Procurement and Technical Standards (PTS) Working Group is chaired by the Office of Finance and Services and includes senior representation from across the NSW Government clusters.

Agencies engage with the PTS Working Group concerning services for inclusion in the ICT Services Catalogue. This drives the development of technical standards, where none exist. The PTS Working Group has the leading role in reviewing and endorsing the technical standards developed in response to agencies’ requirements.

The PTS Working Group is supported by two sub groups responsible for the areas of Telecommunications and Services & Solutions. The sub-groups are responsible for initial development and review of standards relating to their areas of responsibility.

Management and implementation

There is scope to modify standards through the NSW ICT governance arrangements as necessary. Standards are designed to add value, augment and be complementary to, other guidance, and they are continually improved and updated.

This standard does not affect or override the responsibilities of an agency or any employee regarding the management and disposal of information, data, and assets. Standards in ICT procurement must also address business requirements for service delivery.

NSW Procurement facilitates the implementation of the standards by applying them to the goods and services made available through the ICT Services Catalogue. Standards will also be available on the ProcurePoint web site.
**APPENDIX D – NABERS ENERGY RATINGS**

**Minimum NABERS Energy Ratings for data centres**

*As part of the requirements of the Government Resource Efficiency Plan (M2014-08 NSW Government Resource Efficiency Policy) “All data centres will achieve a minimum infrastructure and IT equipment NABERS Energy rating of 4.5 stars by June 2017”.*

NABERS ratings will be obtained for data centres that meet the minimum criteria published by the NABERS program (see [www.nabers.gov.au](http://www.nabers.gov.au)). For the GovDC data centres, the Office of Finance and Services will provide and maintain a minimum 4.5 star NABERS Energy rating. For other data centres, agencies will:

- obtain and maintain a minimum 4.5 star NABERS Energy rating
- migrate to the Office of Finance and Services centralised data centres where the existing data centre’s energy rating cannot be improved to meet 4.5 stars.

Agencies with large portfolios of other building types are encouraged to develop their own energy performance benchmarking system to help improve energy management practices.

**Monitoring**

The Office of Environment and Heritage will collate and maintain a record of NABERS ratings of government-owned and tenanted buildings and data centres. Government Property NSW or the agency, where relevant, will update NABERS Energy ratings if there has been a change in the estimated rating or it has been three years since the last accredited NABERS Energy rating.