Rationale for a Cloud Services Framework

AIIA response to Draft Paper for Consultation

January 2015
About AIIA

The Australian Information Industry Association (AIIA) is the peak national body representing Australia’s information technology and communications (ICT) industry. Since establishing 36 years ago, the AIIA has pursued activities aimed to stimulate and grow the ICT industry, to create a favourable business environment for our members and to contribute to the economic imperatives of our nation. Our goal is to “create a world class information, communications and technology industry delivering productivity, innovation and leadership for Australia”.

We represent over 400 member organisations nationally including hardware, software, telecommunications, ICT service and professional services companies. Our membership includes global brands such as Apple, Avanade, EMC, Google, HP, IBM, Intel, Lenovo, Microsoft, PWC, Deloitte, and Oracle; international companies including Telstra and Optus; national companies including Data#3, SMS Management and Technology, Hills Limited, Technology One and Oakton Limited; and a large number of ICT SME’s.

This submission

The AIIA appreciates the opportunity to provide this response to the Draft Rationale for a Cloud Services Framework, developed by the South Australian Government.

AIIA strongly supports the adoption of cloud services by government and business and is pleased to help facilitate the transition to cloud services by the South Australian Government. As the Draft Framework identifies, take up of cloud solutions is increasing and indeed, ‘mandated’ by some national and international governments.
Comments

The following comments relate to sections in the Draft Framework.

Purpose of this document and current situation
1. AIIA supports the purpose of the document and the overview of the current situation.

Draft Policy Statement
2. AIIA understands the intent to encourage agencies to adopt cloud service models. In our view however, the language of the Policy Statement could be interpreted as punitive. In our experience the following language has proven to be just as effective:
   - “South Australian Government agencies are required to evaluate and implement cloud based services when undertaking any ICT sourcing, procurement or market approach unless it is clear that an alternative solution will deliver a better value, sustainable investment taking into account desired business, innovation and productivity outcomes.”
3. The section would be strengthened by:
   - Clarifying development of the proposed Cloud Services Catalogue.
     - The current text advises that the Catalogue will be created by the agencies and managed by the Office of the Chief Information Officer (OCIO). Notwithstanding, the logistics of how the catalogue will be established and who will actually lead its development is unclear.
     - AIIA supports the establishment of a Cloud Services Panel of recommended cloud service vendors which can be used to support streamlined procurement of services. Such Panels and model supply contracts already exist in some jurisdictions and at the Commonwealth level and could be leveraged by the South Australian Government. Government could engage with industry to develop similar arrangements in South Australia.
   - Ensuring consistency between the Draft Policy Statement and supporting text.
     - The sentence under the heading Encourages Awareness of Cloud Services, which says, “The decision on whether or not a cloud service is selected will still depend on the evaluation process and fitness for purpose with respect to agency outcomes” could be interpreted as undermining the overarching Policy Statement. The language used in this instance qualifies the intended requirement. Agencies could argue that they have ‘special needs’ and that a cloud solution is not fit for their specific purpose. This needs to be avoided.
4. In our opinion, the heading Why ‘cloud first’?, is redundant. If retained it should be clear that cloud services reflect the rise of a new service based procurement model in the area of ICT and reflects an increasing maturity of technology capability and the ICT market.

What are Cloud Services and how are they different
5. AIIA recommends review of the document National Cloud Computing Strategy which provides a succinct explanation of the definitions, benefits, risks and value to government of cloud based services.
6. The section confuses cloud services and shared services. These are not the same and the terms should not be used interchangeably.
   - Cloud services means that a user of a service no longer needs to buy, build, install and operate expensive computer hardware. Users simply access computing resources as a utility service via a ubiquitously available wired or wireless network - from ‘the cloud’.
   - Shared services typically refers to the consolidation of business operations that are used by multiple parts of the same organization - which may be built, hosted and maintained by one of the users but also at the disposable of others. These may or may not also be ‘hosted
services’ which mean the user owns and has full control over all the resources on the available on the server, which may be hosted by a third party.

7. The section could be strengthened by articulating the specific benefits of cloud computing as also outlined in the [National Cloud Computing Strategy](#).

8. The incidental discussion of risk, particularly on page 10 of the Framework (paragraph 2) is potentially inflammatory. A reference to any ‘unfamiliar operational risk’ should be clarified/specified to allay concern.

**Cloud Services Framework**

9. In relation to the proposed Principles, AIIA would suggest the following.
   - For simplicity reword Principle 1 to: *We will accelerate the delivery of innovative service outcomes.*
   - Principle 2 currently insinuates that business requirements will be dictated by available solutions. It is unlikely that Agencies will support this approach. AIIA recommends the following rewording - *We will purchase services that facilitate the achievement of sustainable cost efficient, effective and high quality business outcomes.*
   - Principle 3 could be clarified and strengthened by amending to - *We will develop the expertise and skills to support effective new service procurement models.* This also shifts the focus to appropriate procurement and contract management expertise to support service offerings and procurement paradigms.
   - Principle 4 incorrectly refers to shared service models and the ‘re-use’ of cloud services. This concept is incorrect.
   - Principle 5 similarly refers incorrectly to shared services. In our view the Principle is redundant.
   - We support the focus on communication in Principle 6 but believe that reference to professional project management is a skills issue that should be incorporated into Principle 3.

**Guidelines for Agencies**

10. We would refer you to the excellent work of the Commonwealth Department of Communications - [Cloud Computing Regulatory Stocktake](#), May 2014. This document provides detailed advice regarding the adoption and risk management of cloud based services.

11. Guidelines provided to agencies would, ideally, be supported by appropriate resource material and tools.

12. In relation to Data Security we would provide the following which could be incorporated into your proposed Guidelines document:
   - **Government Cloud Services Require Robust Data Security:** Unsecured network transmitted data is highly vulnerable to breaches
     - Government departments, law enforcement agencies, emergency services, defence agencies and health service agencies hold or have access to an ever increasing wealth of data, including large amounts of personal and sensitive information.
     - While this presents government agencies with significant opportunities for the way agencies develop policy and deliver services to citizens, it also presents government agencies with many challenges, particularly in relation to privacy, as the large data sets could potentially provide an opportunity for unfriendly state and non-state actors to glean sensitive information, or create a mosaic of exploitable information from apparently innocuous data.
   - The Australian Signals Directorate [Strategies to Mitigate Targeted Cyber Intrusions](#) focuses on email, internet,
personal devices and Big Data at rest. However, governments’ large data sets (including sensitive, private, personal and restricted data) traversing Data centres, into the Cloud and between agencies are indisputably targets for criminal and malicious activities, and therefore represent a significant breach vulnerability.

- Given the risks of Big Data breaches, it is therefore imperative that, in addition to adopting a Cloud By Default policy, the SA Government also adopt a ‘Private By Default’ policy and implement a Privacy By Design framework that encompasses the principles of:
  - Proactive not reactive
  - Privacy as the default setting
  - Privacy embedded into design: Cyber Security 2.0 - protecting the breach (the last line of defence) through robust encryption

- Robust encryption of data as it is transmitted across networks would protect the transmitted data if a breach occurs during transmission. Therefore, robust encryption of network transmitted data should be a key component of any effective and comprehensive information security strategy.

13. We would also recommend that Guidelines encourage Agencies to develop a cloud assessment and technology roadmap that includes cloud services as part of an Agency’s ongoing ICT management responsibilities.

14. It would also be appropriate to call out the South Australia Connected reference to innovation and risk taking. This would remind Agencies of the Government’s desire to avoid risk aversion and the focus on risk management. This is important given the negative perceptions of cloud services by some Agencies and encourage them to think more broadly about the government’s overarching policy objectives.

Why does SA need this cloud services framework?

15. In our view this repeats material at the front of the Framework and should either be deleted or integrated in the introductory sections.