DPC/G4.5

GOVERNMENT GUIDELINE ON CYBER SECURITY

ISMF Guideline 5 – Cloud Computing Security Guideline

Background

Cloud computing, and in particular 'Software-as-a-Service' (SaaS), presents the South Australian Government with many opportunities including the potential to reduce electronic storage and internal information and communication technology (ICT) capital investment requirements. However, it also presents potentially significant cyber security risks that require due consideration.

This guideline highlights items of importance that must be considered by agencies contemplating a move to SaaS or other models of cloud computing such as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). This guideline supports implementation of Information Security Management Framework ISMF Policy Statement 5.

Guidance

Cloud computing represents a considerable opportunity for the government and private sector to reduce costs, transfer responsibilities, eliminate duplication and improve service agility and response to change. It is of particular interest to organisations that wish to migrate to an outsourced arrangement for select functions, services or other capabilities that are not considered a component of 'core business'.

Cloud computing carries many of the well documented risks and opportunities associated with traditional outsourcing arrangements, but adds unique dimensions to an organisation's risk profile in terms of liability, control, user access, business recovery and continuity planning, legal obligations, data migration and portability, change management and capacity planning undertakings to name just a few.

Cloud Computing: a heavy duty form of outsourcing

Agencies contemplating a cloud computing implementation in any form should first consult ISMF Guideline 6 to familiarise themselves with fundamental cyber security considerations in procurement activities. This guideline describes additional considerations for cloud computing in recognition of its unique business promise that gives rise to unique business risk characteristics.

Added dimensions to risk assessment

Business owners should conduct a risk assessment for third party suppliers in concert with the agency Information Technology Security Adviser (ITSA) that encompasses the following considerations:

1. Legislative and jurisdictional risk

- where is the service physically located?
- does privacy legislation exist in that jurisdiction? If so, what are the provisions?

2. Terms and conditions of service

- do the terms and conditions confer ownership of the information to the provider?
- do the terms and conditions provide a 'cooling off period' when changes to terms occur?
- under what law and jurisdiction are the terms governed?

3. User and identity management

- how is the identity managed and by whom?
- who has access to the user and account management functions and features of the service?
- is the user identity dedicated to a function and role or is it used for multiple purposes? An example of this is combine private/public activities.

4. Access and connectivity

- is the level of the system availability and accessibility acceptable?
- how is connectivity achieved? Is it encrypted? Does it have redundancy? Does it traverse jurisdictions such as the USA and/or Singapore, China etc?

Alignment with ISMF requirements and ISO 27002 is non-trivial

Owing to the complexity of cloud implementations and the myriad of possibilities it enables, Responsible Parties will need to consider a significant number of policies, standards and controls from the ISMF. The list of ISO/IEC 27002:2006 clauses below establishes a starting point for considered review of these complexities:

- 15.1.4: Data protection, privacy, regulatory requirements
- 11.2: Access management
- 10.7: Media handling and security
- 11.6.2: Separation/Isolation
- 10.7: Operator Procedures
- 10.6.2: Network Security
- 10.10: Logging
- 10.2: Third party service delivery
- 6.2: External organisations

Government Implementation: essential resources

The resources listed or embedded below constitute a minimal reference of documents, tools and utilities that should be consulted in any cloud computing study for South Australian government agencies. Where possible, documents and tools have been embedded with a hyperlink (web location) to the source content so that subsequent versions to those published within this guideline can be acquired. All materials embedded as objects in this guideline remain the property of their respective copyright holders. No rights are transferred or conveyed by using this guideline. All embedded objects have been publicly sourced and rights holders are instructed to contact the Department of the Premier and Cabinet (DPC) if they wish to request removal of their article(s). Embedded objects in this guideline are only accessible in the Word format version of this document (ie not accessible in the PDF version of this guideline).

- Advice on managing the record-keeping risks associated with cloud computing, Australasian Digital Recordkeeping Initiative (ADRI)
- Cloud Controls Matrix, Cloud Security Alliance (CSA), provides accessible translation and lookup between industry and international standards and frameworks with those controls recommended or specified by the CSA.
- Cloud Computing Strategic Direction Paper, Australian Government Department of Finance
- Cloud Computing Security Considerations, Australian Signals Directorate (ASD)
- Cloud Computing Security Risk Assessment, European Network and Information Security Agency (ENISA)
- Security and Resilience in Governmental Clouds, European Network and Information Security Agency (ENISA).

Additional Considerations

Responsible Parties need to recognise that the agility offered by cloud computing can work both ways and that sudden changes may negatively impact business. Agencies should have a remediation plan in place in the advent of:

- adverse or undesirable changes to the terms and conditions of use
- changes of ownership, tertiary provider or merger and acquisitions activity
- changes to foreign and/or Australian legislation (particularly telecommunications interception and privacy)?
- changes in software/user interfaces/technical characteristics or access policies from the provider?
- discontinuation and/or sudden non-availability of the service resulting from legal proceedings, bankruptcy, non-competition etc on the part of the provider.

A risk management process should be used to balance the benefits of cloud computing with the security risks associated with the agency ceding management functions and a large proportion of oversight to a third party.

A risk assessment should consider whether the agency is willing to entrust their reputation, business continuity, and information to an external entity that may erroneously transmit, store and process the agency's data. The risk assessment must consider the criticality and sensitivity of the data involved.

This guideline does not aim to provide the reader with all the responsibilities, obligations, controls or consequences related to secure cloud computing. It is merely an overview of the information provided in relevant cyber security policy and the AS/NZS ISO/IEC 27002 standard. It is highly recommended that agencies review such documents in their entirety. The individual requirements of agencies will have direct bearing on what measures are implemented to mitigate identified risk(s).

References, Links and Additional Information

- Information Security Management Framework
- PC030 Protective Security Management Framework
- Information Privacy Principles Instruction, issued as Premier and Cabinet Circular No12
- Australian Government Protective Security Policy Framework (PSPF)
- Australian Government Information Security Manual (ISM), ASD
- Cloud Controls Matrix, CSA
- Cloud Computing Synopsis and Recommendations, US National Institute of Standards and Technology (NIST)
- Cloud Computing Security Considerations, ASD
- Australasian Digital Recordkeeping Initiative

Document Control

ID	DPC/G4.5
Version	1.3
Classification/DLM	Public I1-A1
Compliance	Discretionary
Original authorisation date	January 2014
Last approval date	February 2019
Next review date	February 2020