SACSF/G3.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline - Engaging Suppliers and Cloud Security

Introduction

Cyber security is fundamental to the successful operations of the South Australian State Government. Cyber security risks are evolving as rapid technological advances lead to an increased reliance on technology to perform critical business functions; and management and effective sharing of information and information technology resources is essential to maintain legal and regulatory compliance, reputational image, and meet the objectives of the State Government.

The South Australian Cyber Security Framework (SACSF) has been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of South Australian Government agencies.

Applicability

The SACSF applies to:

- All South Australian State Government agencies and personnel operating on behalf on the agencies.
- Non-government suppliers and personnel that access South Australian State Government information and resources.

Scope

These guidelines are derived from the requirements of the SACSF. They explain the practices and procedures that South Australian Government agencies are expected to follow when engaging the services of suppliers, contractors or other third parties to access, process, store, or otherwise handle information on their behalf.

Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency.

Supplier access is defined as any local or remote access made by a supplier to Government IT assets. In terms of arrangements with suppliers, the scope extends to the various service delivery interfaces with those suppliers, as defined in contracts and/or service level agreements. It includes auditing of security services implemented by suppliers that have a material impact on the security of information managed by the agency, but otherwise excludes the suppliers' internal processes.

Expectations

In order for an Agency to meet the SACSF expectations for Supplier Management when engaging suppliers, they should ensure they are aware of, and are managing the cyber security risks introduced by the supplier.

Prior to engaging with a supplier agencies should:

1. Perform an assessment of the potential risks introduced by the supplier. A guiding questionnaire to assist with this assessment is available here.
2. Define and document the risk mitigation activities and technical controls required of both the supplier and the agency in a formal supplier agreement. These controls must:
    - Be commensurate with the classification of the information assets to be protected,
    - Align to the agency's risk appetite and risk management framework,
    - Address the system and information access requirements of the Supplier (including any additional third parties providing services to the supplier).
3. Define and document the supplier's assurance reporting requirements based on the agency's risk assessment in a service level agreement (SLA).
4. Ensure the contract / SLA with the supplier is reviewed and approved by the agency or government's legal, procurement or appropriate other representative before execution.
5. Ensure an appropriate non-disclosure agreement is in place.

Obtain evidence of relevant background verification checks of supplier personnel with access to agency information or agency IT assets is provided by the supplier.

During engagement with a supplier agencies should consider:

1. Periodically obtaining evidence from suppliers that they have maintained the required controls as documented in the relevant supplier agreement.
2. Periodically obtaining evidence from the supplier of their cyber security awareness program.
3. Performing periodic vetting of the supplier's competency specific to the role they are performing for the agency in place of internal agency resources.
4. Obtain assurance that the supplier has met their contractual obligations and implemented the controls documented in the SLA.

Upon completing an engagement with a supplier agencies should:

1. Reinforce the supplier's ongoing contractual cyber security obligations, including non-disclosure agreements which must extend indefinitely unless otherwise noted.

Register of Suppliers

Agencies are expected to maintain a register of suppliers providing services that may impact the confidentiality, integrity and availability of agency information and systems. The following is an example of the type of information that should be captured for each supplier:

Description	Example
Description of services provided by the supplier	Support for server infrastructure
Criticality of the service to the agency	High
Agreement information (type of agreement, next review date, reviewer, location of the agreement)	Master Services Agreement last reviewed by [IT Manager] on [DD/MM/YYYY]. [Document location]
Nature of the logical and physical access that the supplier has to agency information	Full physical access to server infrastructure. No logical access – hardware support only
The degree of confidence that the agency has in the security controls and terms in the contract	High
Description of the risks to the business	Unavailability of data centre may result in major interruption to critical services Significant reputational damage
Minimum supplier requirements as documented in the agreement	ISO 27001 certification 99.99% uptime on data centre service Physical and environmental control status reports

Using and maintaining a register will ensure agencies have visibility over who their suppliers are together with their respective security obligations. A supplier register template is available here.

Cloud Security Guidance

Further to the requirements above, this section provides additional guidance with respect to the use of cloud service providers.

Background

Cloud services provide a range of potential benefits for many agencies including cost, scalability, and flexibility of platform and capacity. Using such services may also allow agencies to better focus on their core business, leaving aspects such as IT infrastructure management to specialised service providers.

However, outsourcing introduces different risks to the agency given the loss of direct control over aspects of service delivery, as well as reduced visibility over any breakdown in controls that may occur. Sharing the responsibility between the agency and the cloud service provider may also add to the level of risk, particularly where the separation is not well defined and understood by all parties.

The adopted cloud service model (Infrastructure/Platform/Software as a Service) will impact the responsibilities that are retained in-house and those that are outsourced. In any case, there is potential that neither party will undertake some key activities that fall ‘between’ the stakeholders, and the impact may only become obvious after a serious failure has occurred. The cloud deployment model (Public, private, community or hybrid cloud) may also impact the control options that are available to manage information security risks associated with the service.

Agency Responsibility

Responsibility for risk management remains primarily with the agency, even where activities are performed by a cloud service provider.

Checks and balances must be implemented by the agency to maintain an appropriate level of assurance that the service provider has appropriate processes in place to:

- Manage the security of agency information in line with government policy and expectations, and
- Perform the activities for which the service provider is responsible.

Contractual Considerations

Agencies should ensure that the contract terms with cloud service providers address any data sovereignty issues. Specifically, the terms should establish and agree the location of all agency data held by the cloud service provider, considering:

- The location of the primary data store,
- Replication of data to support high-availability solutions and/or authentication,
- Online and offline backup locations, and
- Administration and support staff who may access the processing environment and data.

The contract should also consider other key issues to the satisfaction of the agency (as the information owner) including:

- Requirements to meet the agency and government requirements (State Records),
- Requirements of South Australian Information Classification System and SACSF R2.0 Storage and Processing of Information in Outsourced and Offshore ICT Arrangements,
- Specification of record keeping functionality and metadata requirements in order to meet regulatory and business record keeping requirements,
- Requirements relating to the storage and use of personally identifiable information meets the requirements of the South Australian Government's Information Privacy Principles,
- Assurance that the cloud service provider cannot use tenant data for applications not specified in the contract. For example, it cannot be on-sold or otherwise used for marketing purposes. It must not be used to data match with databases owned by other clients of the cloud service provider,
- Assurance that no copy of the agency's records or information is retained by the cloud service provider after the termination of the contract (including secure destruction of data in line with records management requirements),
- Requirements for the secure sanitisation or disposal of data storage that has hosted agency data (primary storage and backup media),
- Requirement to advise the agency of any incident that may impact confidentiality, integrity or availability of agency data and allow the agency to manage communications in compliance with SACSF Standard 140,
- Requirement to advise the agency of any changes that may impact data sovereignty,
- Requirements to consult with the agency regarding any third party seeking to have access to tenant records, and
- The legal jurisdiction applicable to any dispute.

The contract must also specify the cloud service provider's obligations at the completion of the contract / on exit from the arrangement, including return of all specified records and associated metadata to the agency in an accessible nominated format(s).

Additional information and references for consideration:

- SACSF R2.0 Storage and Processing of Information in Outsourced and Offshore ICT Arrangements
- Cloud Computing Records Management Considerations
- Cloud Computing Privacy Considerations
- Cloud ICT Services Policy
    - Cloud Services Planning Guidelines
    - Cloud Services Network Guideline
    - Cloud Services Financial Guideline
    - Cloud Services Information Sheet

Document Control

ID	SACSF/G3.0
Version	V1.0
Classification/DLM	OFFICIAL
Compliance	Discretionary
Original authorisation date	November 2019
Last approval date	November 2019
Next review date	November 2020

Licence

With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a Creative Commons Attribution (CC BY) 4.0 Licence. To attribute this material, cite Department of the Premier and Cabinet, Government of South Australia, 2019.