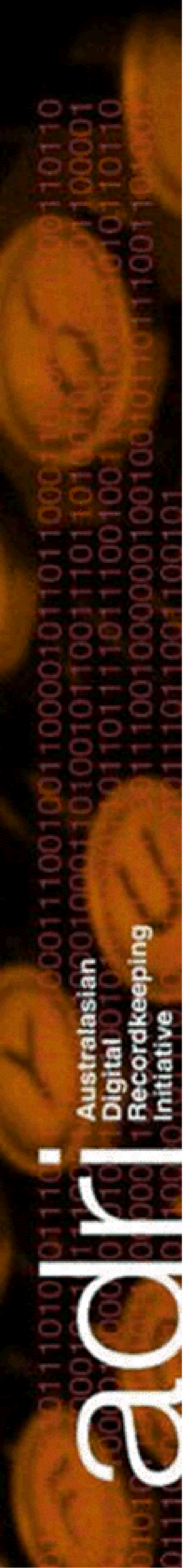

CAARA
Council of Australasian Archives
and Records Authorities

IM requirements for SAAS

Consultation Draft

November 2019

Table of Contents

1 Introduction to Consultation Draft

1.1 Background

Many organisations are entering into **Software as a service (SAAS)** arrangements to take advantage of the cost savings and the many potential benefits they offer. Commonly these arrangements are used to outsource the provision of software that staff use to do their jobs every day, including office tools (e.g. Office 365), email (e.g. Gmail), finance and personnel systems (e.g. SAP).

From an information management perspective, the key feature of SAAS arrangements are that the organisation's information (data, records) is held on external systems that are not controlled or managed by the organisation. While this has some advantages over traditional software installation, the organisation's legal and practical responsibilities do not change because the information is now being held in a service provider's datacentre. The organisation is still subject to privacy, security, freedom of information and public records requirements, so careful consideration must be given to information management requirements when setting up these arrangements to ensure that the organisation complies with all its obligations.

ADRI was concerned that there was not a formal, structured, method of considering IM requirements when State and Federal governments were entering into SAAS agreements and as a consequence there was a serious risk of government information using SAAS arrangements being poorly managed over time.

1.2 The proposed solution

This document looks at SAAS requirements from an Information Management (IM) perspective. It provides a checklist of IM considerations that must or should be covered in a SAAS agreement. The checklist is provided as a guide to 'best practice' in Information Management in SAAS systems.

Its intended audience is:

- IM staff who need guidance in the application of IM principles to SAAS systems
- IT staff and project decision makers

This document is not a complete guide to procuring a SAAS arrangement. It focuses on the IM aspects that should be considered to effectively manage the information throughout the SAAS arrangement and beyond to meet legal and operational requirements.

1.3 This document

This document is a draft for comment on the IM requirements for SAAS arrangements. It has been prepared by a sub-committee of the Australasian Digital Recordkeeping Initiative (ADRI) composed of representatives from State and Federal Archives from Australia and New Zealand. ADRI is a key work program of the Council of Australasian Archives and Records Authorities (CAARA).

1.4 Consultation process

We would especially like people with experience of SAAS procurement, information managers, and archivists to comment on the draft IM requirements.

2 IM checklist for SAAS procurement

2.1 Purpose of this checklist

This checklist provides a list of Information Management (IM) considerations that should be covered in any Australian Federal or State Government Software as a Service (SAAS) agreement in order to manage the information held in the SAAS system in a way that meets legal and operational requirements. It can be used to conduct risk assessments and research into the suitability of SAAS products.

2.2 Background

Many Australian government organisations are entering into **Software as a service (SAAS)** arrangements to take advantage of the cost savings and the many potential benefits they offer. Commonly these arrangements are used to outsource the provision of software that staff use to do their jobs every day, including office tools (e.g. Office 365), email (e.g. Gmail), finance and personal systems (e.g. SAP).

From an IM perspective, the key feature of SAAS arrangements are that an organisation's data (information, records) is held on external systems that are not controlled or managed by the organisation. While this has advantages over traditional software installation, a Government organisation's IM legal and practical responsibilities do not change because the data is now being held in a service provider's data centre. The organisation is still subject to privacy, security, freedom of information and public records requirements, so careful consideration must be given to IM requirements when setting up these arrangements to ensure that the organisation complies with all its obligations.

This document focuses on the application of information management (IM) requirements in SAAS systems. It lists a series of requirements and tasks that, when completed, will ensure that the SAAS procurement team understands and has addressed the IM implications of an SAAS agreement.

2.3 Scope of the checklist

This checklist covers Information Management issues in SAAS agreements, it does not cover the full range of issues that a SAAS agreement must address. For a more comprehensive guide to developing SAAS contracts see DTA's Cloud Assessment tool .

2.4 Audience

The intended audience for this checklist is:

- IM staff who need guidance in the application of IM principles to SAAS systems
- IT staff and project decision makers

3 The Checklist

3.1 Definition of SAAS

For the purposes of this document, SAAS (Software as a Service) is any arrangement where a vendor uses their cloud infrastructure and cloud platforms to provide customers with software applications. (Definition from Australian Cyber Security Centre *Cloud Computing Security Considerations*)

3.2 General principles

Information created, managed and hosted using a Software as a Service (SAAS) arrangement must remain:

- authentic, accurate and trusted;
- complete and unaltered by unauthorised means;
- secure from unauthorised access;
- secure from unauthorised deletion;
- findable, readable, usable and re-usable; and
- related to other relevant information.

3.3 Legal position of information held in SAAS systems

An Australian State or Federal Government organisation has the same legislative and policy obligations to protect and manage its information, regardless of where it is stored.

Entering into an SAAS agreement requires special consideration of information management functional requirements as you will need to identify what obligations the organisation has to protect and manage its information under various pieces of legislation, regulations, Government policy or agency policy.

Such legislation includes, for example,

- Privacy Acts, such as the Commonwealth Privacy Act 1988
- Archival Acts, such as the Commonwealth Archives Act 1983 or the state equivalents
- Legislation specific to data, such as the General Data Protection Regulation or Victorian Health Records Act 2001.

3.4 Checklist Part 1: Information access

In order to carry out your business, your organisation needs continued access to its information. This access will typically continue long after the SAAS agreement has terminated. The people who need this access may not only include the front-line staff carrying out the business, but also managers, others supervising and auditing the business, and external clients.

The questions to be considered in this section involve establishing whether access to information held in the SAAS can be maintained at all times during the period of the agreement and after the agreement terminates.

Information Access Checklist
Check ownership and rights over information. Typical questions: • What are the vendor's rights or ownership of your data, and will these have any practical effect on your ability to use the information? • Does the agreement give the SAAS vendor (or anyone else) any rights over the information held in the SAAS system (e.g. permission for the vendor to retain the information)? • Is all the information entered in the SAAS (or created by the SAAS system) owned by your organisation?
Check jurisdiction in which the information is held. Typical questions: • Is any of the information being held outside your legal jurisdiction; in particular, is it being held outside Australia? • If so, are their legal or policy implications due to potential foreign access to the information? • What are the difficulties of any legal dispute outside your jurisdiction (e.g. costs, contractual protections over information may be consequently be effectively unenforceable)?
Check the disaster recovery regime offered by the SAAS vendor. • Is the disaster recovery plan for the SAAS system appropriate? • Is the plan regularly reviewed and exercised? • What is the residual risk of information loss (e.g. a loss of information due to a failure that was not prevented by the disaster recovery regime)? Note that no disaster recovery regime is perfect, and the residual risk should be compared to the residual risk of in-house operation.
Check the business continuity regime offered by the SAAS vendor. • Is the business continuity plan for the SAAS system appropriate (e.g. plan for outages)? • Is the plan regularly reviewed and exercised? • What is the residual risk of continuity failure (i.e. a failure to be able to conduct business despite execution of the business continuity regime)? Note that no business continuity regime is perfect, and the residual risk should be compared to the residual risk of in-house operation. • What is the risk of the SAAS vendor suddenly ceasing to supply the service (possibly involuntarily, e.g. by bankruptcy), and what is the plan if this occurs?
Evaluate the agreed security incident response. • Is the security incidence response plan for the SAAS system appropriate? • Is the plan regularly reviewed and exercised?

3.5 Checklist Part 2: Information management

The information needs to be managed effectively while it is held in the SAAS system. These management functions ensure that the information (records) are authentic, reliable, and have integrity; essentially that they can serve as evidence.

The tasks in this section involve establishing what management functions are supported by the SAAS system.

Information Management Checklist

Check what mechanisms are provided to ensure the integrity of the information.

- Does the SAAS system have the ability to store information in such a way that it cannot be modified after creation, or, if it can be modified, the modifications are automatically tracked?
- Have you developed an ongoing management plan for the information: description, access, retention, protect, store, preserve and disposal of information?
- Can you export the information periodically or as required into a format that allows you to interrogate the data (ie a business intelligence tool, spreadsheet)?

Check the ability to be able to organise the information.

- Does the SAAS system have the ability to link related records together (including links to records held outside the SAAS system)?
- Does the SAAS system have the ability to organise and describe the records?

(Note it may not be necessary to organise the information in a classic recordkeeping fashion, such as in a business classification system; the organisation of the information may be tailored for the particular business that the system supports.)

Check the access control over the information.

Does the SAAS system have sufficient ability to control access to the information based on business requirement?

3.6 Checklist Part 3: Information privacy and security

Organisations have obligations to keep information held by them private and secure regardless of where it is held. Obligations vary depending on the type of information but the same rules apply to Information held in SAAS systems, just as much as they apply to in-house organisational systems.

The tasks in this section first involve establishing the sensitivity of the information being held in a SAAS system, and then establishing the threats to the information.

Information Privacy and Security Checklist
Evaluate the sensitivity and security requirements of the information that is to be held in the SAAS system. Issues that should be considered are: • What information is to be held in the SAAS system? • What privacy and security legislation or policies control access and use of this information? In particular, confirm the sensitivity of the information (e.g. Confidential, Secret) and ensure that the SAAS system has been validated against this sensitivity level. • What would be the consequence of a release of the information from the SAAS system? Note: not all information will be suitable for storage in SAAS systems due to legislative or policy restrictions. Requirements for the Commonwealth (and general requirements for States) are found in The Australian Government's Protective Security Policy Framework and the Information Security Manual.
Evaluate what access to the SAAS system (and the information it contains) is given to people or organisations related to the vendor (eg staff, contractors, allied companies) and what controls are in place over this access. Access could include the ability to monitor operations on the information. Issues to consider include: • What checks and vetting processes (eg employment checks) are performed by the SAAS vendor to ensure that their employees and subcontractors will respect agreements on access to the information held in the SAAS? • Does the SAAS vendor use sub-contractors to deliver all or part of the SAAS system? Are there appropriate, enforceable, agreements with these sub-contractors to ensure the security of the information stored in the SAAS system? Are these agreements audited? • Does the agreement with the SAAS vendor allow information held in the SAAS system to be shared with a third-party (this could include derived data, such as statistics or summaries)? Under what circumstances is this allowed? • Does the agreement with the SAAS vendor allow the information held in the SAAS system to be used by the SAAS vendor for its own purposes or benefits (e.g. data mining)? Does this access violate the sensitivity or security requirements of the data? • Does the SAAS agreement explicitly prohibit the SAAS Vendor and subcontractors from doing anything that would breach the Information Privacy Principles (IPPs) or any other relevant legislation, standards or policies (e.g. Protective Security Policy Framework and the Information Security Manual). • Is tracked data anonymized so that your specific information is not handed out in an identifiable manner?
Evaluate what legislative access the SAAS vendor must support. Issues considered include: • Do the laws of the jurisdiction in which the SAAS system and/or SAAS vendor exist allow third party access to the information held in the SAAS system (eg for security purposes)? • Under what circumstances could this occur and who may have access? • Does this access violate the sensitivity or security requirements of the data?
Check what technical controls are in place over the information while being held by the SAAS vendor and while it is in transit to or from the vendor's systems. • Does the SAAS vendor use technologies to create a secure gateway environment, for example firewalls, traffic flow filters, content filters, antivirus software? • Does the SAAS vendor use Australian Signals Directorate (ASD) approved cryptographic controls to protect data in transit and at rest in the SAAS system? • Does the SAAS vendor use physical security processes, products and devices that are endorsed by the Australian Government or relevant State Government?

- Can the SAAS vendor assure that the virtualisation and multi-tenanted storage arrangements secure and segregate data appropriately?
- Does the SAAS vendor use identity and access management systems for users to log in? For example, do the applications support multi-factor authentication? What is the access recovery procedure?
- Can the SAAS vendor ensure that data isn't aggregated in storage in such a way that it increases its sensitivity?
- How often are security updates and patches applied
- What will the vendor do where physical media is damaged and replaced, requirements for the sanitisation or deletion of data in the damaged media
- Is the hosting in an Australian based IRAP assessed datacentre?

3.7 Checklist Part 4: Information return

An inevitable consequence of negotiating a SAAS agreement is that the arrangement will eventually end. The arrangement may be replaced by a new SAAS arrangement with a different vendor, the software may be brought in-house, or discontinued when the agreement finishes. The key issue for an organisation is maintaining accessibility and useability of the information after the agreement has ended when the organisation no longer has access to the SAAS software. The key to service continuity is the return of information from the SAAS system in an accessible and useable format.

The tasks in this section involve establishing whether you can effectively retrieve the information held in the SAAS for continued use or archiving once the SAAS agreement terminates. *Effective* retrieval means that the information is returned in a usable format, in a reasonable timeframe with no additional costs.

Information Return Checklist

Confirm the how information will be returned to you at the end of the agreement. Typical questions involve:

- When will information be returned to you (information must be returned at the termination of the agreement, and should be returned whenever required)?
- How will the information be returned to you (over the network, or by physical media), and how secure is this?
- How long will the return of information take (for example, a large quantity of information may take days to download over the Internet)?
- Who is in control of this process (you or the vendor), and is there provision for dealing with problems or bugs in the process?
- Can the return process be tested (periodically during the course of the agreement, or in the lead up to the end of agreement)?
- How much flexibility do you have in the return process (to vary the process depending on your needs)?
- Are the details of the return fixed in the agreement, or left open?
- Is the agency able to export data from the SAAS system at other times (eg transferring valuable digital records into State custody as part of a planned transfers program)?

Confirm the format(s) in which the information will be returned to you at the end of the agreement. Typically, there will be a range of information to be returned – for example, information content (e.g. documents), databases, metadata and logs – linked together in complex ways. To be useable by your organisation (or by a replacement SAAS vendor), this information must be returned in a format (or a set of formats) that can be accessed using tools that your organisation has.

- Have you agreed data exchange standards? Specify the format of the information and associated metadata is to be returned to your agency and processes to be followed when information is migrated. Preferably the provider should use open formats to support readability over time.
- Are the format(s) the information is returned documented, and will you have an accurate, up-to-date, usable copy of the documentation (especially note any legal impediments to use of the documentation – e.g. supplying a copy to a competitor of the SAAS vendor)?
- Does your organisation have staff with appropriate skills to migrate and remediate the information if needed?

Can you ensure that a copy of the information does not remain in the SAAS vendor's possession after return?

- Information could be held in back-up or recovery copies, secondary data centres, or un-erased on media.
- Are media sanitation methods considered appropriate by the Information Security Manual? Sanitation may need to extend to destruction of physical hardware on which such data is held to avoid risk that the data may be recovered.

Confirm your approach to exporting information out of the SAAS system

- Do you need an ETL (Extract, Transform, Load), API or other software to help migration or ingest of data?
- Can you export a full manifest of system holdings prior to destruction – so that data indexing and searching technologies can be used to scan the system.
- Can you use 'machine learning' software for automated mapping of data structures to facilitate exporting data to another system?

Evaluate what tools you will be able to use to verify the operation of a SAAS vendor. Issues to be considered include:

- Will you be able to use your organisation’s existing tools for integrity checking, compliance checking, security monitoring and network management?
- Does the vendor provide for and maintain system audit logs that provide confirmation that required information protection requirements are being met?
- What requirements are imposed on the SAAS vendor to notify you a security incident?
- What are the time frames to notify you after the security incident is detected?
- What are the time frames for clarifying the significance and effect of the security incident?

3.8 Checklist Part 5: Information retention and disposal

There are legal requirements specifying the minimum period of time information created by your organisation must be kept. Some information can be disposed of quickly while other information must be kept for long periods of time – ranging from several years up to permanently.

The tasks in this section involve identifying the minimum retention period of the information held in the SAAS system and determining if, and how, information that can be disposed of, will be.

NOTE: you may need to discuss these tasks with an ICT specialist

Information Retention and Disposal Checklist
Evaluate the need for the SAAS system to support disposal of records. Issues to be considered are: • Determine the minimum retention period of the information held in the SAAS system. • Determine if it is likely that information will need to be disposed of from the SAAS system (given the SAAS agreement length). • Determine if it is likely to be an issue if the information is retained for longer than the minimum retention period (e.g. it is sensitive or secret).
Evaluate the disposal mechanisms built into the SAAS system. • Dos the system implement any ad-hoc disposal mechanisms (e.g. storage quotas that enforce deletion, or administrative functions that purge information at will). Note that enforced deletion may make the software unfit for purpose. • If it is necessary to dispose of records from the SAAS system, does the system support the necessary disposal functionality? (This should include related functionality, such as disposal freezes). • Determine if the SAAS system can implement holds (eg in the event of legal action). It may be appropriate for the SAAS system to have no disposal mechanisms (eg if the information has a longer retention period than the expected life of the SAAS agreement, or if the information is sufficiently non sensitive or open that retention past its disposal point is acceptable).
Can you ensure that any storage media disposed of by the SAAS vendor has been properly sanitised? • Are media sanitisation methods aligned with the Information Security Manual? Sanitisation may need to extend to destruction of physical hardware on which such data is held to avoid the risk that the data may be recovered. • What are the residual risks of the disposed data? (eg How are back-up and recovery copies of the disposed data handled?)