Information Management Requirements for Software-as-a-Service

Version 1.0 May 2020

adri Australasian Digital Recordkeeping Initiative

CAARA
Council of Australasian Archives and Records Authorities
follow #caara

The Australasian Digital Recordkeeping Initiative (ADRI) is composed of representatives from all state and national archival authorities in Australia and New Zealand. ADRI is a Working Group of the Council of Australasian Archives and Records Authorities (CAARA).

Table of Contents

1 Introduction

1.1 About this document

This document provides a checklist to highlight information management (IM) issues that an Australian government organisation must consider when selecting and managing a **Software as a service (SaaS)** deployment. These issues must be addressed to ensure compliance with Australian law, government policy, and best practice.

The checklist contains five parts that cover different aspects of IM in the SaaS deployment lifecycle and the information lifecycle. These are: information access; information management; information privacy and security; information return; and information retention and disposal.

The checklist can be used to conduct risk assessments and research into the suitability of SaaS products.

It does not cover the full range of issues that a SaaS agreement must address. See the Digital Transformation Agency's Cloud Assessment Tool for a guide to developing SaaS contracts that addresses these other issues.

We want this to be a living document, and would be grateful for suggestions as to ways to improve the usability and effectiveness of future editions.

1.2 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[1].

1.3 Background

Many Australian government organisations are entering into SaaS implementations of business systems. 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 IM perspective, the key feature of SaaS arrangements is that an organisation's information (data, 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 information 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.

1.4 Audience

The intended audience for this document and checklist is:

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

[1] Australian Cyber Security Centre, 2020, *Cloud Computer Considerations*, viewed 8 May 2020, https://www.cyber.gov.au/publications/cloud-computing-security-considerations.

1.5 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.

1.6 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 a SaaS agreement requires special consideration of IM 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:

- 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*.

1.7 How should you use the checklist?

Agency staff should use the checklist to select and review SaaS deployments.

The checklist can be used in the preparation of selection criteria that vendors must respond to as part of the selection process. It can also be used to inform members of selection panels that do not have an IM background about IM requirements on government information that affect SaaS deployments.

After implementation of a SaaS system, the checklist can be used in the regular review of the effectiveness of a SaaS deployment.

The checklist should also be used in conjunction with other checklists that cover non-IM SaaS issues.

We have prepared this document to focus on the aspects of SaaS deployment we have expertise in. Other resources should be consulted to cover the full range of requirements that a SaaS deployment must meet.

1.8 Why have we made these recommendations?

The Council of Australasian Archival and Records Administrations (CAARA) 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.

1.9 Who made these recommendations?

This document was prepared by a sub-committee of the Australasian Digital Recordkeeping Initiative (ADRI). ADRI is composed of representatives of the State, Territory and National Archives of Australia and New Zealand operating as part of CAARA.

The sub-committee would like to thank all those people who provided input and feedback during the development of the recommendations.

2 The Checklist

2.1 Part 1: Information Access

In order to carry out your business, your organisation needs continued access to its information. This need for access will typically continue long after the SaaS agreement has terminated. The people who need this access will not only include the front-line staff carrying out the business, but also managers, people 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 system can be maintained at all times during the period of the agreement and also after the agreement terminates.

Information Access Checklist
Check the ownership and rights over information. Does the SaaS vendor (or anyone else) have any rights over, or ownership of, your information, and will these have any practical effect on your ability to use the information? *In some circumstance, rights over your information may not be an issue. For example, many social media SaaS platforms require a non-exclusive license over any information loaded into them. If the information has been publicly released, this license may cause no issues.* Is all the information entered in the SaaS (or created by the SaaS system) owned by your organisation?
Check the disaster recovery regime offered by the SaaS vendor. Does the disaster recovery plan for the SaaS system reduce the risk of information loss to an acceptable level? Is the plan regularly reviewed and exercised? What is the residual risk of information loss (i.e. 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. Does the business continuity plan for the SaaS system reduce the risk of loss of access to the information (and the duration of loss of access) to an acceptable level? 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)? What is plan if the SaaS vendor suddenly ceases to supply the service? *This cessation may be involuntarily, e.g. by bankruptcy.* What is the risk that this could occur? *Note that no business continuity regime is perfect, and the residual risk should be compared to the residual risk of in-house operation.*

2.2 Part 2: Information management

Your information needs to be managed effectively while it is held in the SaaS system. Among other things, these management functions ensure that the information (records) are authentic, reliable, and have integrity. Without these characteristics, the information will lose value 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 documented?
Check the ability to be able to organise the information. Does the SaaS system have the required ability to link related information together (including links to information held outside the SaaS system)? *The required ability depends on the needs of the business application. In some applications the linkages between information may be only within the SaaS system, in others it may be required to link to information held in external systems, such as an EDRM system.* Does the SaaS system have the ability to organise and describe the information? *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.*
Evaluate what tools you will be able to use to verify the operation of a SaaS vendor. 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 to provide confirmation that required information protection requirements are being met?
Check the jurisdiction in which disputes will be is held. Is the jurisdiction in which disputes will be held outside your legal jurisdiction? In particular, is it being held outside Australia? If so, will there be any difficulties in the event of a legal dispute? *For example, legal costs may mean that contractual protections over information would be effectively unenforceable.*
Check the management plan for the information. Have you developed an ongoing management plan for the information? Such a plan includes description, access, retention, protection, storage, preservation, and disposal of information. Can you export the information periodically, or as required, into a format that allows you to interrogate the information? *The export may be to a business intelligence tool or spreadsheet.*

2.3 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 obligations 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 and security classification of the information being held in a SaaS system. This sensitivity and security classification then controls the required degree of protection against the threats to the information.

Information Privacy and Security Checklist
Evaluate the sensitivity and security classification (or other security requirements) of the information that is to be held in the SaaS system. What information is to be held in the SaaS system? What privacy and security legislation or policies control access and use of this information? Confirm the sensitivity and security classifications of the information (e.g. Confidential, Secret) and ensure that the SaaS system has been validated against these levels. 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 the access control over the information provided by the SAAS system. Does the access control system provided by the SaaS system have sufficient preciseness to control internal (agency) access to the information based on business requirements?
Evaluate what access to the SaaS system (and the information it contains) is given to people or organisations related to the SaaS vendor (e.g. staff, contractors, allied companies) and what controls are in place over this access. What checks and vetting processes (e.g. 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 between the vendor and the 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? *Sharing could include derived information, such as statistics or summaries.* Under what circumstances is sharing allowed? If sharing is allowed, does the sharing violate the sensitivity or security requirements of the information? 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)? If access is allowed, does the access violate the sensitivity or security requirements of the information? 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)? Does the SaaS vendor track users of the service (e.g. cookies), and, if so, is the tracked information anonymised so that information about your users is not handed out in an identifiable manner? *Note access could include the ability to monitor operations on the information*.

Information Privacy and Security Checklist
Evaluate what external access to your information the SaaS vendor must support by legislation. Is any of the information being held outside your legal jurisdiction. In particular, is it being held outside Australia? Is the SAAS vendor outside your legal jurisdiction. In particular, is it primarily or wholly located outside Australia? 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 (e.g. for internal security purposes)? Under what circumstances could this occur and who may have access? Does this access violate the sensitivity or security requirements of the information?
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 information 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 information 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 information is not aggregated in storage in such a way that it increases its sensitivity? *For example, combined with other information with the effect that de-anonymises information.* How often are security updates and patches applied to the SAAS systems? Is the SAAS hosting in an Australian based Information Security Registered Assessors Program (IRAP) assessed datacentre?
Evaluate the agreed security incident response. Will the security incidence response plan for the SaaS system: • notify you immediately a security incident occurs that may or does affect your information? • allow you to understand the nature of the security incident and the effect on the information held and your stakeholders? • allow you to communicate promptly and effectively with your stakeholders about the incident and the consequences of the security incident? • satisfy the legislative and policy requirements that apply to your organisation in the event of a security incident (including required timeframes for actions)? • recover or mitigate the effects of the security incident? Is the plan regularly reviewed and exercised?

Information Privacy and Security Checklist

Ensure that any storage media disposed of by the SaaS vendor has been properly sanitised.

What happens to media once it is no longer being used to hold your information?

Media could have held the operational copy of the information, back-up or recovery copies, or copies at secondary data centres.

Media could be no longer in use due to 1) routine replacement of degraded or failed media; 2) reduction in storage capacity required; 3) disposal of information (see Part 5); or 4) return of information at the termination of the agreement (see Part 4).

Given the sensitivity and security classification of the information, are the media sanitation methods to be used considered appropriate by the Information Security Manual?

Sanitisation may need to extend to destruction of physical hardware on which information was held to avoid the risk that the information may be recovered.

2.4 Part 4: Information return

An inevitable consequence of negotiating a SaaS agreement is that the arrangement will eventually end. When the agreement is finalised, the arrangement may be replaced by a new SaaS arrangement with a different vendor, the system may be brought in-house, or the system decommissioned. The key issue for your organisation is maintaining accessibility and useability of the information after the agreement has ended—when you no longer have access to the SaaS software. The key to access and 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 system 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.

When will information be returned to you?

Information must be returned at the termination of the agreement (unless it is disposed of - see the next part), and should be returned whenever required.

Are there any charges or costs for returning your information?

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 before the formal end of the agreement? *Testing may occur 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 at the time?

Are the details of the return fixed in the agreement, or left open?

Is the agency able to export information from the SaaS system at other times (e.g. transferring valuable digital records into State custody as part of a planned transfers program), and what charges will be made for this?

Information Return Checklist
Confirm the format(s) in which the information will be returned to you at the end of the agreement. Have you and the SaaS vendor agreed on information exchange standards? Has the format of the information and associated metadata to be returned to your agency been specified? Have the processes to be followed when information is returned been specified? Are the format(s) the information will be returned in documented, and will you have an accurate, up-to-date, usable copy of the documentation? *Especially note any legal impediments to use the documentation, e.g. can you supply 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? *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. The provider should use open formats to support readability over time.*
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 information? Can you export a full manifest of system holdings prior to destruction? *This allows information indexing and searching technologies can be used to scan the system.* Are there tools for automated mapping of data structures to facilitate exporting information to another system?

2.5 Part 5: Information retention and disposal

There are legal requirements specifying the minimum period of time that 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 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.

There are several approaches to implementing information retention and disposal. These include (but are not limited to): the SaaS system providing formal retention and disposal functionality; managing retention and disposal when migrating from one SaaS system to another; or transferring the information to a formal records system. The best approach will be determined by the information retention and disposal requirements and the functionality provided by the SaaS system.

Information Retention and Disposal Checklist
Evaluate the need for the SaaS system to support disposal of records. What is the minimum retention period(s) of the information held in the SaaS system? Is it likely that information will need to be disposed of from the SaaS system? Will it be an issue if the information is retained for longer than the minimum retention period (e.g. it is sensitive or secret)? *The information held by a SaaS system may have different retention periods.* *It may be appropriate for the SaaS system to have no disposal mechanisms (e.g. 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).*
Evaluate the disposal mechanisms built into the SaaS system. If disposal is required, does the system implement an effective disposal mechanism? Does the system implement any ad-hoc disposal mechanisms? *Ad-hoc disposal mechanisms include storage quotas that enforce deletion, and administrative functions that allow information to be purged at will.* *Inappropriate ad-hoc disposal mechanisms may make the SaaS system unfit for purpose.* If it is necessary to dispose of information from the SaaS system, does the system support the necessary disposal functionality? *This should include related functionality, such as disposal freezes.* Can the SaaS system implement holds (e.g. in the event of legal action)?