Cloud application (software as a service agreement)

From report 20: 2018/9 – Information Systems Audit Report 2019

Office of the Auditor General
Serving the Public Interest

In a software as a service (SaaS) arrangement, responsibility for cyber security is shared between the vendor and customer. Public sector entities remain responsible for security including governance and access to information. Entities should assess the risks associated with handing over data to vendors and ensure sufficient controls are in place to meet each entity's security needs, including that contracts include measures to mitigate risks and protect information held in the cloud. Ongoing contract management is also essential and should include the entity verifying that the vendor adheres to agreed terms. This may occur through third party assurance reports and entity reviews.

The following table shows some better practice principles entities should consider when choosing a SaaS provider and considerations for ongoing contract management. This is not intended as an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre[1].

Stage	Principle	Our expectation
Decision to adopt SaaS	Understand risks	Perform a risk assessment to understand security risks associated with handing over information to a cloud vendor. The sensitivity, use and value of data should inform an understating of the risks to be closely managed when weighing value for money considerations
	Vendor	Knowing who the vendor is and what they do. Vendor reputation and its compliance with recognised security standards should be assessed. The Australian Cyber Security Centre maintains a list[2] (CCSL) of Australian government certified cloud vendors
SaaS contract and management	Security	Appropriate controls should be defined to protect the application and existing ICT systems that interact with the application from cyber attacks
	Data sovereignty	Data is subject to the laws of the country where it is stored. Entities should prefer an arrangement where data is stored in Australia. If this is not possible, the nature of data going overseas and laws of those countries should be carefully considered
	Data ownership	Contracts should clearly state who has legal ownership of any data during and after the contract
	Data retention and deletion	Contracts should clearly define the data retention method and period
	Access to data and monitoring	Controls to restrict and monitor access to data should be in place
	Vendor lock-in	Controls to enable efficient migration of data to other cloud or on premise systems, should be defined. An exit strategy should be agreed with the vendor to support the move

[1] https://www.cyber.gov.au/publications/cloud-computing-security-considerations

[2] https://acsc.gov.au/infosec/irap/certified_clouds.htm

Stage	Principle	Our expectation
	Encryption of data	Appropriate levels of encryption should be defined for data in transit and at rest. This should also include management of the data encryption key
	Data segregation	Many SaaS applications provide access to multiple customers on a shared platform. Controls should be in place to segregate data from other tenants
	Security breaches	Contracts should clearly define how the vendor must report security breaches and include penalties and indemnities. Entities should have access to relevant evidence (e.g. logs) for forensic investigations
	Availability of application and data	Data backup requirements should be defined and vendor disaster and business continuity plans should meet the entity's business needs. Contracts should define acceptable down times and penalties. An appropriate escrow agreement should be considered if the SaaS application is built or highly customised for the entity
	Strong authentication controls	Access to cloud applications and data should have strong controls and include multifactor authentication
	Assurance reports	Vendors should provide independent audit assurance reports (e.g. SOC 2) to confirm vendor controls meet expectations and operate effectively
	Right to audit	Contracts should define the entity's right to conduct a security audit of vendor controls to protect the confidentiality, integrity and availability of applications and information
	Background checks	Vendors should perform background and criminal history checks for their staff. Security clearances should be considered for highly sensitive data
	Ongoing contract management	Vendor compliance with agreed terms should be regularly checked.