Cloud services

Information and records management considerations

December 2018

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND
Part of the Department of Internal Affairs

New Zealand Government

Document details

Document Identifier: 18/G15

Version	Date	Description	Revision due
0.1	Oct 2018	Development draft	
1.0	Dec 2018	Published	Dec 2021

Contact for enquiries

Government Recordkeeping Directorate
Archives New Zealand
Phone: +64 4 499 5595
Email: rkadvice@dia.govt.nz

Licence

CONTENTS

1 Overview

Cloud based services are any internet based IT services where the organisation's information and records are created, stored and/or managed. They are increasingly used by public sector organisations in New Zealand, as they offer efficient and cost-effective solutions. These benefits must however be weighed up against the risks associated with privacy, security, and information and records management.

This document outlines considerations for organisations' decisions on using cloud based services.

2 Government 'cloud first' policy

The New Zealand government requires public sector organisations to accelerate their adoption of cloud services — in a balanced way — so they can drive digital transformation. The 'cloud first' policy requires organisations to:

- adopt cloud services in preference to traditional IT systems
- make adoption decisions on a case-by-case basis following a risk assessment
- only store data classified as RESTRICTED or below in a cloud service, whether it is hosted onshore or offshore.

Requirements for public sector organisations when adopting cloud services have been issued by the Government Chief Digital Officer (GCDO). Public sector organisations must undertake an information risk assessment of cloud services, including privacy and security issues, following GCDO guidelines. The aim of this assessment is to systematically and regularly check, identify, analyse and mitigate all risks in a service level agreement or contract.

3 Use of the cloud in relation to the Public Records Act

The use of cloud based services to create, store and manage information and records does not diminish or remove the statutory responsibilities of public sector organisations in relation to the *Public Records Act 2005* (the Act) and the mandatory *Information and records management standard*. The requirements apply to information stored in a cloud based service.

Therefore it is critical for information and records management staff to be involved in the cloud provider assessment process and the final decision-making, to guarantee the organisation meets the legislative requirements of both the Act and the mandatory standard.

4 Assessing the risks

While the risk assessment process may seem lengthy, it is important for organisations to remember that the choice of a cloud provider is ultimately their decision, and therefore their responsibility to dedicate time and resources to it. Information and records management knowledge is required to ensure that information and records management requirements are taken into consideration during the assessment process.

A cloud service provider should be able to answer questions regarding functionality, reliability, availability, security, privacy, information and records ownership/stewardship, integration and customisation.

Information management staff must be involved, with others, in the initial risk assessment and planning as well as during business-as-usual operation. Once an organisation has started with a service provider, it needs to make sure that there is a process in place for regularly monitoring how well the information and records management needs of the organisation are being met by the cloud services used.

Key considerations for using cloud services are outlined below.

5 Assessment: key things to check in relation to information and records management

The key questions listed below are indicative only; organisations should consider whether there are any additional questions that reflect their specific circumstances.

Key considerations	Recommendations	Key questions
Content	The value, importance and sensitivity of the information and records to be held in the cloud should be accurately assessed to ensure it is adequately protected. Risks should be assessed based on content or subject matter of the information and records and the level of sensitivity and importance to the business of the organisation.	○ *What kind of information and records will be created?* ○ *What is the level of sensitivity?* ○ *Have they been identified for long-term retention?* ○ *Have they been classified open or restricted access records under the Act?*
Ownership	Information and records outsourced to a cloud environment should remain the legal and intellectual property of the organisation.	○ *Does the contract clearly specify ownership of information and records?* ○ *If the service provider subcontracts parts of their operation to other providers, is ownership of the information and records documented and understood by all involved parties?*

Key considerations	Recommendations	Key questions
Location of provider	Assess, with help of legal experts, the jurisdictional risk of using a cloud provider based off shore, as it is likely to be subject to the law of the host country, and legislation may be different. Follow the advice of the jurisdictional assessment documentation provided by the GCDO: https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/jurisdictional-risks/ If the provider is not able to support the requirements of the New Zealand legislation and standards in relation to information and records management, the organisation may be unable to comply with its New Zealand regulatory requirements. For organisations with stewardship for iwi and hapū information and records, extra consideration should be given to their location.	○ *Where will the information and records be stored/hosted?* ○ *Which legislation, or other jurisdictional requirements, will the information and records become subject to?*

Key considerations	Recommendations	Key questions
Protection, Security and Privacy	Information and records in the cloud are more exposed to unauthorised access; more so if the cloud service provider subcontracts parts of its operation to other companies. Therefore organisations should assess the cloud provider against the risk of illegal release of information, and level of reputation damage that this could cause. Also information and records stored and managed in a cloud environment must be protected from unauthorised deletion or alteration. Check the way information and records will be managed and accessed by third parties, especially if there is personal information involved. Where information and records have access restrictions, the organisation must ensure these are managed appropriately in the cloud environment.	○ *What kind of security framework is provided?* ○ *How does the provider prevent unauthorised disposal?* ○ *Will the organisation be consulted regarding a third party seeking access to its information and records?* ○ *If the provider stores the organisation's information and records with those of another organisation, what kinds of controls are in place to guarantee secure partitioning?* ○ *How are access and identities of users managed?*
Business continuity	Take business continuity into consideration when assessing the risks; check that back-ups are accessible at all times, and the cost involved retrieving information from those back-ups. As cloud services are provided over the internet, it is more likely that there may be some periods of service disruption where information and records are inaccessible. For critical activities where access to information and records is essential, the impact of loss of access even for a short time may be severe.	○ *Is there a business continuity plan in place in the event of an incident/outage?* ○ *What are the practicalities of it? And the cost?* ○ *Are the information and records discoverable at all times, no matter what?*

Key considerations	Recommendations	Key questions
Portability and Interoperability	Check that proprietary interfaces and programming languages used by cloud service providers won't create barriers to migrating information and records to another environment. Also system updates should be applied with detailed consultation with every organisation or individual using the system, so there is no loss of control over the integrity of information and records. In a cloud environment, a lack of portability standards may make it hard to remove business information and records to meet retention requirements at contract termination. To avoid the evidential nature of the records being compromised an organisation must be able to prove that records could not have been altered in any way while stored in the cloud; otherwise this will negate their value as evidence.	○ *What are the processes in place for migration, and how information and records will be accessible and readable after the migration to another provider?* ○ *What is the level of interoperability between the different cloud applications used by the organisation?* ○ *What is the possible impact of system updates on the integrity of information and records?* ○ *Does the cloud system have the ability to easily migrate the information and records to another environment?* ○ *What is the impact of migration decisions by the cloud provider on the reliability and completeness of information and records, and associated metadata?*
Metadata	Information and records created, stored and managed in a cloud environment must be able to link with their relevant metadata, providing context and thus ensuring their reliability as evidence.	○ *Have the minimum requirements for metadata been applied?* ○ *Have the information and records been classified in accordance with the organisation's business classification schemes?*

Key considerations	Recommendations	Key questions
Search, audit and reporting functionalities	Information and records hosted in the cloud should be easily discoverable for information requests, as the Official Information Act 1982 and the Privacy Act 1993 legislation applies regardless of the location of information and records. Reporting functionality should also be considered to facilitate internal and external audit processes. The evidential value of information and records may be affected if appropriate audit trails and descriptions of management processes performed on records while in cloud systems are not maintained.	○ *What are the cloud provider's capabilities for search across information and records?* ○ *What kind of reporting and audit trail functionality exists?* ○ *Will information and records remain easily and quickly discoverable for audits, legal inquiry or release?* ○ *Is the provider able to report easily on the management and use of the records, and provide sufficient information about it?* ○ *Are the cloud services auditable?*
Preservation	To ensure information and records are maintained for as long as required by the organisation, consider if the format will allow for continued accessibility long term. Preservation methods, software, system and/or infrastructure used by the provider must be carefully assessed.	○ *What kind of preservation activities will be performed by the provider to guarantee the information and records remain accessible and usable overtime?* ○ *Does the preservation activity performed include metadata as well?*

Key considerations	Recommendations	Key questions
Disposal	Use of cloud services is not a form of disposal. Organisations need to monitor the retention, disposal and transfer of the records held in the cloud. While disposal coverage is not a prerequisite for signing-up with a cloud service provider, it is strongly recommended to apply the disposal authority (DA) at the point of creation when using a cloud service. Also organisations should check how easy it is to update those settings when changes to the organisation's DA occur. For public offices, records held in the cloud must have retention periods and the disposal action of either 'destroy' or 'transfer to Archives New Zealand' applied to them. Providers are not necessarily bound to follow the organisation's disposal schedule retention periods and could unintentionally expose the organisation to greater litigation risk and lead to additional costs, by retaining information and records longer than the disposal schedule prescribes. Conversely, information and records intended for long term retention might be illegally deleted or overwritten by the provider's server, thereby breaching the Act. There is also the risk of information and records not being disposed of in a timely manner, after authorisation by the organisation. It is common for service providers to replicate records for multiple backup, sending copies to sites in different locations or even different jurisdictions. This can mean that information and records due for destruction are not properly deleted from every server held in every site, which poses a serious risk for information and records such as those containing personal or sensitive information. Providers must delete and digitally 'shred' when required by a disposal schedule. Certificates of destruction should be asked for.	○ *For public offices, what export / extract functionality will be available (bulk/individual items, drag and drop) when long term / permanent value information and records are due to be transferred to Archives New Zealand?* ○ *How will you confirm the destruction of files from servers not under your direct control?* ○ *Can the cloud service offer destruction of information and records due for destruction (including any copies) in a manner that ensures that the information and records are not able to be reconstructed?* ○ *How much resource will be needed from the organisation to confirm destruction by the cloud service provider?* ○ *Are the retention periods for backups aligned with organisational retention periods?*

Key considerations	Recommendations	Key questions
Termination of contract	The contract terms and conditions should state that, if the contract is terminated, the information and records will be returned in a useable form, and removed permanently from the service provider's systems. Check that the contract includes specific details about termination, and fate of information and records hosted.	○ *The obligations of the cloud provider should be specified in the contract.* ○ *What are the conditions if the organisation terminates the contract? Will the organisation be stuck, or locked-in (information lock-in, platform lock-in, tool lock-in), with their current provider because of the complications and costs of switching to a new provider?* ○ *Is there a clause specifying that the terms cannot be changed in regards to IM requirements when a provider is declared bankrupt, sold to a new service provider or terminates its services?* ○ *If necessary, can the information and records be easily migrated to another provider, without the integrity of the information and records being compromised?* ○ *In the event that a provider is changed, would the new provider have an obligation to honour the conditions in the previous contract? Would the organisation be guaranteed continued access to their information and records?* ○ *What format will the information and records be exported back to the organisation in (such as an open format), and how long it will take before the information and records can be accessed again following termination of the contract?* ○ *What costs would be involved for the organisation?* ○ *If the service provider enhances your information and records in the cloud, will you also get a copy of those? Or is the agreement solely for the original versions?* ○ *Will the service provider be required to keep the information and records on its systems during a transition period?*