Cloud Computing and Records Management

Introduction

Cloud computing is the practise of using internet-based servers to store, manage and process records throughout their lifecycle. Cloud computing poses both benefits and risks to government institutions. Cost savings and gains in efficiency, accessibility and flexibility must be weighed against risks associated with security, privacy and information management. A risk assessment should be undertaken to identify and manage jurisdictional, governance, privacy, technical and security issues before engaging a cloud service provider and records management concerns must be addressed.

When considering using a cloud service provider, consultation throughout the institution is essential and must include information technology, records management, legal and individual business units.

Public records created, stored and managed in the cloud are subject to *The Archives and Public Records Management Act.* The Act defines public record as "a record made or received by a government institution in carrying out that government institution's activities". Government institutions are responsible for managing the storage, access, transfer or destruction of public records as per the Act.

This document outlines some information and records management concerns which should be addressed by government institutions when considering the use of cloud-based computing services.

Issues to consider

The following records management issues must be considered when deciding whether to engage a cloud service provider:

1. **Scope**
   The types of records that are to be stored on a cloud server must be carefully considered. The types of records and their content will determine the necessary levels of security controls, preservation and migration strategies that will be applied. Records must be stored in a secure format and the government institution must ensure that confidential and sensitive information is afforded the level of data protection required by applicable legislation such as *The Archives and Public Records Management Act,* FOIPP and HIPA. Also, the cloud service must be able to provide the appropriate level of data protection as required.

2. Ownership

Ownership of public records stored in the cloud must be retained by the Government of Saskatchewan. Cloud service providers that allow for ownership by entities other than the Province should not be considered.

3. Server Location

Storage location must be specified as a requirement when procuring a cloud service provider. Records which are to be stored on a server outside of Saskatchewan or outside of Canada must be examined carefully to ensure that they will be managed in accordance with Saskatchewan laws. Records stored on a server which is maintained outside of Saskatchewan may be subject to the laws of that jurisdiction. Any contract negotiated with a cloud service provider must address any risks associated with storing the information outside of Saskatchewan. The contract will need to address the protection of confidentiality and the security of the information, the application of Saskatchewan laws to the service provider, insurance requirements and indemnification from potential liability. The solicitor advising the government institution should be consulted to assess the risks and to review any contractual arrangements.

4. Preservation

Information stored in the cloud must be preserved in formats which ensure that it remains accessible and useable in accordance with approved records schedules. Service providers must afford migration strategies which meet the institutions needs and integrity checks must be conducted on a regular basis to make sure that the data remains accurate and consistent.

5. Retention and Disposal

Protocols must be in place by the service provider to ensure that records which have met their retention requirements are destroyed only upon instruction from the government institution. Government institutions are required to follow the records disposal process administered by the Provincial Archives of Saskatchewan. Information deemed to have historical value must be stored in a format that is consistent with that required for transfer to the Archives. Evidence must be made available by the service provider that records which are not being acquired by the Provincial Archives of Saskatchewan are deleted from the cloud server when they have met their retention requirements. This includes all electronic copies, including back-ups.

6. Security

Information must be stored in a secure format, with all meta-data intact, complete and unchanged. Records must retain their ability to provide evidence of business transactions. Adequate safeguards must be in place to protect personal information and other sensitive and confidential records and to prevent security breaches. Cloud

service providers must ensure that they have proper back-up and disaster recovery protocols in place.

Any contract with a service provider must clearly specify who has access rights to information stored in the cloud. The information stored in the cloud is the property of the Government of Saskatchewan and should only be accessed by those persons who require access to manage the information. The service provider should be required to document any access to these government records.

7. Cloud Server Reliability and Service Continuity

Cloud service providers must have protocols and procedures in place to address the integrity of the records in the event of any problems or incidents which may occur (such as the server shutting down or the service provider going out of business). Risks associated with remote access should also be addressed by the provider. The provider must be able to return complete records as required by the government institution in the event that they are no longer able to deliver the service and the data must remain accessible, transferable and usable. These issues should be addressed in any agreement entered into with a service provider.