Cloud Services

Role of Data Trustee in Cloud Acquisition Process

October 24, 2019
Agenda

- Objective
- Context
- Risks & considerations
- Process highlights
- Your role
Objective

- Describe what **Cloud Services** are
- Explain the **pros and cons** of Cloud Services
- Discuss the proposed role of **data trustees** in the Cloud Acquisition process
- Develop common decision-criteria for data that will live in the cloud
What are Cloud Services?

Instead of running a software application and storing/accessing your data on your desktop or on McGill’s network, this is provided to you remotely as a service (by an external service provider) and accessed over the Internet.

- Reduces costs of maintaining our systems
- Allows for quicker implementation times
- Provides us with additional flexibility to connect to the university anywhere, anytime

There is a significant number of cloud solutions in use at McGill, and this number is increasing rapidly.

- Since our data is no longer kept within the walls of our organization, we don’t have the knowledge or control of who has access to our data without performing due diligence.
Finding

Process to acquire/use cloud services **not formally documented/communicated**

Acquisition/use of cloud services **without understanding the risks associated**

Use of cloud services **not managed consistently**

Action plan

Actions are underway **since May 2019 and planned until December 2020 (and beyond)** to ensure the processes are clarified and key stakeholders are informed.
Risks

Risk of **non-compliance with laws and regulations**

Risk of acquiring cloud services whereas a comparable solution is already available

Risk of getting locked into a contract that does not fulfill your needs
Highlights of Cloud Services Acquisition Process

This process applies to both free & paid cloud services!

Steps 2, 4, 5 & 6:

1. Assess your needs (requester/user)
2. Contact Data Trustee(s) for concept approval
3. Submit Procurement Mandate Form
4. Privacy Assessment
5. IT Risk Assessment
6. Contract Assessment
7. Final Decision

Note: This is an extract from a more detailed process
Cloud Service Acquisition Process - Detail

**Needs Assessment**

1.1 Defining Needs
   - 1.1.1 Obtain approval
   - 1.1.2 Consolidate analysis results
   - 1.1.3 Assess Data Request
   - Data in Scope
   - Procurement Mandate
   - Approved in concept
   - Reject

1.2 Determining Strategies
   - 1.2.1 Decide award method
   - 1.2.2 Confirm requirements
   - Privacy Options

**Obtaining Proposals**

1.3 Obtaining Proposals
   - 1.3.1 Distribute documents
   - Request Data Flow
   - Privacy Notice
   - Completed Privacy Addendum
   - ITRQ
   - Completed ITRQ

**Selecting contractor**

1.4 Selecting contractor
   - 1.4.1 Obtain contractor approval
   - 1.4.2 Issue Request for Proposal
   - Not approved
   - Approved

**Contracting**

1.5 Contracting
   - 1.5.1 Attend contract approval
   - 1.5.2 Issue contract
   - File contract
   - End
Requestor considerations for all Cloud Services

Before

- Have you defined your needs?
- Will you be able to adapt your processes to the solution?
- Are you really dealing with cloud services?
- What kind of data could be accessible to the provider or other 3rd parties?
- Does McGill already have a similar, vetted solution?

During use & at renewal

- Resources and expertise are available to support the ensuing maintenance and monitoring of the cloud services
- Changes to scope are assessed from a privacy and security perspective
- Significant changes to laws, regulations and industry standards are reviewed for compliance
- Service issues with vendor are addressed
- Vendor changes to processes, systems, or « flow of data » are evaluated
- Breach of contract related to security, performance or privacy compliance are addressed to McGill’s satisfaction
Which data is confidential?

**Regulated** institutional data
- Data protection/use is mandated by law, regulation or industry requirement
  
**Public** institutional data
- Non-confidential information
  
**Protected** institutional data
- Data that is not regulated, nor public
- Data protection/use is governed by contract or McGill rules

**Examples**
- Personal information
- Student/employee records
- Passwords
- Legal files

- Press releases
- Public access website pages
- Published documents, ex. brochures, annual reports, academic calendars, campus maps, course descriptions, etc.

- Internal memos
- Meeting minutes
- Documents incl. proprietary information
- Research grant applications
- Etc.

*Note: Research data is subject to the same Cloud data classification.*
Proposed Data Trustee Role at McGill

You are responsible...

For a sub-set of Enterprise data in your functional area

To promote proper access, accuracy, privacy, integrity, security and availability of the data

For activities of Data Custodians in your functional area

For strategic planning, policy, and oversight of your data

Data trustees would need to have global oversight of their data
Data Trustee Role in the Cloud Process

The data trustee is responsible to **assess the appropriateness** of sharing the data in the Cloud for a specific need.

- Evaluate the business need to assess if **data should be propagated** outside of McGill.
- Understand whether cloud solution will **host authoritative data** ("source of truth").
- Ensure consistency with **policies / orientations**.
- Keep abreast of **security breaches**, both at McGill and at other organizations.
- Make a decision in accordance with **process and criteria**.
- Consider the **effects on the reputation** of McGill or individuals.
- Understand the **scope of data** to be stored or accessed in the cloud.
Privacy addendum

- McGill developed the privacy addendum to be able to comply with data privacy legislation.

- It entails contractual clauses to ensure that our vendors respect privacy obligations.
  - The addendum takes precedence over contractual clauses.

- Data hosting locations and data access locations are key elements in the privacy addendum.
## Cloud Acquisition Process - Tools available

<table>
<thead>
<tr>
<th><strong>Cloud Services 101</strong></th>
<th>• A basic introduction to cloud services explaining what it is, the benefits and risks as well as the expectation of the requestor’s role in the process.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud Process</strong></td>
<td>• High-level overview of the Cloud Service Evaluation Process, for anyone at McGill planning to acquire or use a cloud service.</td>
</tr>
<tr>
<td><strong>Cloud considerations</strong></td>
<td>• A set of questions for the requestors to ask themselves as a guideline prior to the acquisition, during the use, and at renewal of a cloud service.</td>
</tr>
<tr>
<td><strong>Cloud directive &amp; guidelines</strong></td>
<td>• The official document that prescribes when and where you can store (and transmit) McGill data, depending on data security and privacy needs.</td>
</tr>
</tbody>
</table>

Visit our web page: [https://mcgill.ca/cloud-directive](https://mcgill.ca/cloud-directive)
We need to take ownership!

We are all responsible for the security of McGill’s data!

This does not only concern Procurement or IT Services.

We all have to adhere to process and perform due diligence.

We need to become pro-active and work together.

We need to protect sensitive data in the cloud.

Your role as a data trustee is critical for protecting McGill’s institutional data.