INTRODUCTION

This document describes Simon Fraser University’s cloud computing strategy. This strategy defines our approach for assessing cloud computing opportunities and risks by weighing the potential value against the full cost of ownership that incorporates security, privacy law compliance, and life cycle management costs (including capital, licensing, support and evergreening).

Our strategy encompasses two distinct perspectives:

**Cloud Services Consumer**

- Adopt cloud computing services that provide maximum business value to the University while avoiding or minimizing potential risks.

**Cloud Services Provider**

- Leverage our new Water Tower Building Data Centre improvements to:
  - Enhance and expand SFU’s support for high performance research computing.
  - Position SFU as a potential shared services provider in alignment with provincial and federal government initiatives.
  - Pursue revenue-generating opportunities with new business partners.

CLOUD COMPUTING OVERVIEW

Cloud computing is driving change in how IT services are delivered. Over the last few years it has been the subject of much debate within both the information systems and business communities. The speed and flexibility of cloud resources can shorten time to deployment in development and production environments. Researchers are increasing their use of cloud-computing resources for computationally intensive research and analysis of large data sets. Faculty, students and staff are embracing easily accessible and low-cost cloud-based services such as file storage and synchronization. SFU needs a strategy to address how it will approach this changing environment.
Essentially, cloud computing is a group of servers running software used by a community of users. While there is nothing special about the technology itself, the physical deployment and ownership of the technology presents a more challenging debate. There are several different ways of deploying cloud computing:

**Private cloud**

A locally hosted offering where the data and services reside on servers that are located on the physical premises of the client organization. The services and data are accessible by any authenticated user located on the organization’s network or through secure access to the organization’s network. For example, SFU’s private data storage cloud service, SFU Vault, runs on servers that are managed in our IT Services data centres.

**Community cloud**

An externally hosted offering where the data and services reside on servers that are located outside the physical premises of the organization. These services and data are accessible by users that belong to a specific group of related organizations. The community is a group with shared interests local to a specific area, such as a province, and so would not be constrained by provincial legislation. An example from British Columbia would be the cloud services developed by BCNET. All the services are hosted within the province and are managed by a provincial non-profit organization. A broader geographic example is WestGrid (hosted and supported by SFU), which provides a community cloud service for the western provinces.

**Hybrid cloud**

A combination of locally-hosted and third-party-hosted cloud services. Typically, data is stored locally and processed somewhere else. An example is what IBM is attempting in Canada to avoid the distribution of Personally Identifiable Information (PII) outside of Canadian boundaries.
Public cloud

Services and data reside on servers located in data centres managed by a third party or publicly owned company. These services and data can reside anywhere in the world. An example is Google’s Gmail service.

Of these four models, the community, hybrid, and public clouds are all explicitly outsourcing strategies. In these models external organizations do work previously performed inside the University on a fee for service basis. We need to be cautious about staffing and union issues when moving work to external organizations.

Each cloud deployment model can provide three different types of services: software, platform, and infrastructure.

Software services

Cloud based software services provide software on a subscription model. The service provider owns and hosts the software and provides it to users on a subscription basis. This model is the all-in-one cloud computing service. In this case the outsourcer manages all aspects of the information system; the client does not do software development and does not need a data centre. An example of this model is SFU’s FluidSurveys service.

Platform services

Cloud based platform services provide computing resources and tools to enable software development. These services include operating systems and hardware. The service provider owns and hosts the equipment and development tools. Clients use these resources to create their own software applications. We do not have an example of this type of system at the University, but Amazon provides this type of service.
**Infrastructure services**

Cloud based infrastructure services provide access to data centres with servers, storage, backup, operations staff, and networking technology. The service provider owns and manages the equipment and provides it to users on a subscription basis. In this model the outsourcer manages the basic technology infrastructure and does not manage any application or operating system software. These types of service providers have been available since the 1960s.

---

**Cloud Computing Risks**

Cloud computing and personal mobile devices are the key disruptive technologies behind the mobile, social-media-aware, always-on, real-time society that is developing. However, cloud computing is not yet an established service environment—many facets have not stabilized and present significant risk and hidden or unknown costs. Often, return on investment assessments of cloud based services do not factor in these risks and costs and vendors are reticent to promote awareness of these issues.

In addition, cloud computing suppliers promote their services as providing a high-performance, service-rich environment that can bring agile IT services to the enterprise at reduced cost. Organizations assessing cloud computing opportunities are often caught up in the excitement of new technology and ignore the full spectrum of issues. They typically move to cloud computing because of business cases that are incomplete and that ignore the true total cost of the outsourcing service. These assessments inevitably ignore the many potential risks that accompany cloud computing use. Some of these risks are as follows:

**Significant information security risks**

There is growing uncertainty about the storage of PII data on servers affected by foreign legislation. Canadian legislators and the public are becoming increasingly sensitive to foreign data storage issues, yet U.S. owned cloud vendors express frustration in supporting our national interests.
Immature technologies

Despite vendor claims, cloud solutions such as the Desire2Learn learning management systems do have major failures and these failures have resulted in significant teaching issues for several Canadian universities.

In many cases, cloud vendors have refused to accept contractual liability for loss of data required by Canadian Freedom of Information legislation.

Ephemeral service offerings

Cloud vendors will shut down their service if it is not profitable. There is no clear legal recourse to recovering your data and services in these circumstances.

In an emerging environment, acquisition of smaller companies by larger companies is common. For example, SFU currently uses FluidSurveys for research and other surveys. Since many of our surveys include PII data, the University specifically selected this product because it was owned and operated by a Canadian company. Recently, the company was purchased by a foreign organization. What happens to our data now?

When depending on externally provided services, we need to carefully plan exit strategies. What will happen to our data if we no longer subscribe to the service? For example, any data stored in a different jurisdiction could potentially become the property of that jurisdiction and they could be entitled to keep it forever. Texas is an example where this occurs. We need to negotiate full repatriation and deletion clauses for all of our data and address who pays for repatriation and deletion of the data.

Lack of an established legal framework

Costly legal fees are required to establish the provision, operation, succession, and retirement of cloud services. Complex and sometimes expensive contract negotiations have delayed the implementation of certain cloud services in many Canadian universities.

In addition, there is an opinion that the control of one’s PII is a human right. This argument has not been tested in Canadian courts but legal scholars are growing more convinced that this opinion will have to undergo judicial review.
Labour concerns

Outsourcing of IT work is a traditional area of concern of staff unions and they have already shown interest in bringing their concerns into the collective bargaining process at other universities. Also at other Canadian institutions, faculty associations have brought protection of private data cloud computing concerns to negotiations. In our assessment of any cloud solution we must be cognizant of any potential labour issues.

Faculty concerns

Protection of intellectual property in the cloud is hampered by widely disparate legislation in countries where cloud vendors host systems. Research that is deemed acceptable in Canada is not always considered acceptable in other jurisdictions. Information hosted in other countries could, indirectly, place researchers at personal risk outside Canada's borders.

Network concerns

Network performance across the Internet is outside the control of the University. Any cloud computing business cases must consider what happens if Internet connectivity is degraded or lost entirely. Furthermore, increased Internet network bandwidth is required to support the larger data transfer required by strategic cloud services and the costs associated with this may be significant.

Despite claims of superior security capabilities by vendors, their assertions cannot be applied to the network connectivity between the University and Internet service providers, leaving a weak link in the cloud security model.

Future service cost concerns

Outsourcing services to the cloud is much easier than repatriating these services back in-house. Currently, cloud service providers are offering attractive financial incentives for organizations to move their IT services to the cloud—in some cases services are offered free of charge. Once IT services have been migrated to the cloud, organizations will be in a relatively weak negotiation position should service providers decide to increase the cost of their services.
Operating versus capital budget focus

A factor often overlooked is that external cloud computing services will move the University’s cost base from a capital intensive position to one that is heavily operational cost based. This significant change requires assessment from a funding perspective and the potential impact on the financial structure of the institution. Although most private sector businesses welcome a move to operational expenditures, much of the University’s funding for information systems is capital based. Outsourcing information systems services to cloud computing services will demand a shift from capital budget to operating budget funding.

These risks, like cloud computing itself, are still evolving and maturing. Adopting externally-based cloud computing requires careful consideration of these risks, weighed along with the true total cost of ownership of the solution.

Once all these costs and risks are assessed, an exit strategy must be developed. The reality of cloud computing is that any outsourcing decision needs to be revisited regularly just as any other information systems decision needs to be revisited as the business needs change. There needs to be a clear exit strategy if the cloud service no longer meets the business needs, environmental factors (e.g. laws) change, the service is acquired by a foreign company, or the cloud service provider goes out of business. The costs associated with implementation of a back-out strategy might also be significant.

CLOUD COMPUTING STRATEGIES

There are two core strategies required:

1. How will SFU behave as a cloud services consumer, and
2. How will SFU behave as a cloud services provider.

Most universities are only concerned with how they will consume cloud services provided by other organizations. At SFU we have a rich history of providing cloud services to other organizations such as BCcampus and BCNET. Our future includes providing large scale cloud services on a national scale. Significant investments at SFU by Compute Canada in
high performance computing require us to provide community cloud services as a national research infrastructure initiative.

**Cloud Services Consumer Strategy**

As a cloud services consumer, the University is adopting a strategy of Private Cloud Preferred. This strategy enables us to avoid outsourced cloud computing issues associated with data privacy risks, base budget funding, and union concerns. The University has recently implemented a private cloud service (SFU Vault) on our own infrastructure that makes use of industry standard technologies to provide an agile, secure, redundant environment to host our own services and applications. SFU Vault is an SFU owned and managed private cloud service that replaces high-risk foreign public cloud services such as Dropbox.

Adoption of community, hybrid or public cloud services can proceed if our analysis validates these services as mature, all costs are considered, the residual risk is acceptable, and they are determined to be clearly the best option from a business perspective. The University will consider cloud technologies in the following order of preference:

1. **Private Cloud**
   
   Our primary preference is to implement cloud solutions in our private cloud if the full business case justifies this choice.

2. **Community Cloud**
   
   We will always give preference to solutions residing in our province, then within Canada, in order to minimize jurisdictional issues.

3. **Hybrid Cloud**
   
   We will consider specific targeted solutions for applications, software, or platforms in a hybrid cloud environment on the condition that data resides on one of our campuses on University owned systems and transfer of information for processing does not put PII data at risk.

4. **Public Cloud**
   
   We must recognize that despite the risks there are cases where public cloud solutions may be the best, and sometimes only option.
CLOUD SERVICES PROVIDER STRATEGY

As a cloud services provider, we will leverage SFU's investment in the new Water Tower Building Data Centre to enhance and expand our capability as a community cloud service provider for high performance research computing across the province and country. We are currently a community cloud service provider for Compute Canada and will position SFU as a potential shared services provider in alignment with provincial and federal government initiatives. We will also pursue revenue-generating opportunities with new business partners.

We will manage the following services to ensure our private cloud services meet or exceed national high performance computing expectations:

- Scalability of physical infrastructure (power, cooling, space, backup power)
- Information security
- Operations support
- State of the art technological expertise

RETURN ON INVESTMENT ASSESSMENT

IT Services will develop a cloud service assessment methodology to guide University business units through the process of gathering information about a proposed cloud solution. It will help in the assessment of: the sensitivity of the information, the consequence of its compromise, and the acceptable level of risk. These assessments will help to determine if the risk of moving information to a community, hybrid, or public cloud is reasonable given the identified return on investment.

For any cloud service, a Threat and Risk Assessment and Privacy Impact Assessment will be performed to determine the overall risk exposure to the University. Information on how to perform this process is available from the Privacy Office or from IT Services. Once the risk is understood along with an appreciation for the total cost of ownership, an appropriate business case can be developed to guide the cloud service decision process.
NEXT STEPS

While cloud computing continues to evolve and mature, our next steps include:

- Continue with our strategy of Private Cloud Preferred.
- Require all cloud computing service agreements and contracts for SFU to be reviewed and approved by IT Services.
- Develop a policy for outsourcing information systems based on this strategy paper.
- Establish a contract review process for any cloud computing service.
- Use our internal cloud service capabilities to grow and develop our One I.S. priorities.
- Enhance our identity management system to support the expanding cloud environment.
- Continue to improve the security of our data and manage its access.
- Be open to adopting cloud services that deliver a true benefit to the University.
- Continue to observe and track the development and maturation of community, hybrid, and public cloud services.
- Continue to develop our Water Tower Building as a world class cloud computing data centre.
- Pursue opportunities to enhance and expand our community cloud service offerings.

CLOUD OPPORTUNITY EVALUATION METHODOLOGY

One of the key components of the University’s cloud strategy is a repeatable process for evaluating opportunities and ensuring that a total cost of ownership model is used that incorporates a true cradle-to-grave costing approach. This methodology includes the following steps:

1. Review business requirements
   a. Service catalogue additions
   b. Business support
2. Evaluate service
   a. Identify benefits
   b. Prioritize available services
   c. ID delivery/service options

3. Perform a risk assessment
   a. Threat and risk assessment
   b. Privacy impact assessment
   c. Control identification
   d. Statement of residual risk
   e. Compliance strategy

4. Calculate true total cost of ownership
   a. Capital costs
   b. Operational costs
   c. Adoption costs
   d. Exit costs
   e. Retirement costs
   f. Risk mitigation costs
   g. Compliance costs
   h. Estimate benefits/process savings/return on investment
   i. Develop business case

5. Determine overall requirements
   a. Service level agreements
   b. Engagement, backup, and exit strategies
   c. Project charter development

6. Enterprise Architecture compliance
   a. Cloud deployment model options analysis
   b. Initial operating condition (IOC) definition
c. Enterprise architecture compliance assessment

7. Acquisition
   a. Service model options analysis
   b. RFP if appropriate/vendor evaluations
   c. Service contract assessment and management

8. Implementation
   a. Change management
   b. Data migration
   c. Data security
   d. IAM integration
   e. Infrastructure integration
   f. Initial operating condition (IOC) achieved

9. Support
   a. Standards/Services
   b. Metrics/Reviews
   c. Monitoring/Continuous Compliance

10. Service Retirement/Replacement
    a. End of life determination
    b. Retirement/Replacement decision
    c. Data retrieval
    d. End of service life

ACKNOWLEDGEMENTS

This strategy has been guided by research that other institutions have implemented.