# BENEFITS AND RISKS OF ADOPTING CLOUD-BASED SERVICES IN YOUR ORGANIZATION

**MARCH 2020** **ITSE.50.060**

This document introduces the benefits and the risks of using cloud-based services, which deliver computer processing capabilities as a service rather than as a product. Cloud service providers (CSPs) provide on-demand and scalable computing environments. Overall, cloud-based services offer your organization more flexibility than on-premises IT solutions. Cloud-based services can also provide your organization with a richer set of capabilities and free up your organization's IT resources. However, using cloud services does not automatically ensure that protections are applied to the assets that fall under these services. With cloud services, your organization's senior decision makers are still accountable for protecting the confidentiality, integrity, and availability of IT services and information. Your organization should identify all business and security requirements and manage all associated risks.

## CLOUD SERVICE MODELS

**Software as a service (SaaS)**: Your organization purchases the use of applications that are hosted by the CSP, with little to no visibility on the underlying infrastructure.

**Platform as a service (PaaS)**: Your organization creates and runs custom applications, but the CSP provides the facilities required to build, deliver, and support applications and services.

**Infrastructure as a service (IaaS)**: You can access fundamental computing resources (e.g. servers, data storage, networking equipment) and use the CSP's equipment to deploy and run the software that your organization needs.

## BENEFITS OF CLOUD COMPUTING

Cloud-based services provide your organization with a richer set of capabilities and can free up your organization's resources. Depending on the level of service you select, the CSP is responsible for hardware needs, internal labour, and maintenance costs.

Some benefits include the following examples:

- Services can be rapidly and automatically scaled up or down to meet your organization's demand.
- Services are subscription-based so that you only pay for what you use.
- IT services are rolled out without having to go through time-consuming internal procurement, development, and implementation processes.
- Less of your organization's IT budget is spent on developing and maintaining software and infrastructure.
- Valuable space associated with off-site servers is recovered and costs (e.g. maintenance, electricity, cooling, licensing) are reduced.
- CSPs are responsible for the security of the cloud.

## RISKS

When your organization adopts cloud services, you give up direct control over many aspects of security and privacy. Despite this lack of control, your organization is still accountable for protecting the confidentiality, integrity, and availability of its IT services and information based on legal, regulatory, and business requirements. Although the implementation of security protections may be facilitated by moving to the cloud, your organization's senior decision makers remain accountable for managing risks associated with these services.

Before using cloud services, you should take the following considerations into account:

- Potential violations of or non-compliance with legal and regulatory restrictions and requirements (e.g. Canada's *Privacy Act, Personal Information Protection and Electronic Documents Act,* and *Direction for Electronic Data Residency*, the European Union's *General Data Protection Regulations*).
- Impact to the resources associated with moving, consolidating, or standardizing your organization's on-premises IT services so that you can use cloud-based services.
- Loss of direct control and visibility of cloud components.
- Lack of security personnel in your organization who are familiar with cloud-based deployments.
- Possible confusion related to roles and responsibilities, if not clearly defined, when responding to incidents.
- Potential of being locked in to a cloud service, including your financial obligations and your ability to move to another service provider.

**Your organization is accountable for securing and maintaining assets IN the cloud.**

**EXECUTIVE SERIES**



## CSP IT SECURITY ASSESSMENT PROGRAM

The Canadian Centre for Cyber Security (Cyber Centre) stood up a CSP IT Security Assessment Program in which we evaluate a CSP's security processes and controls against a baseline set of our recommended security requirements. Note that while we review the CSP's processes and existing controls, your organization is responsible for determining your security requirements and ensuring that the CSP you choose to work with is capable of meeting those requirements. You can use the outputs of our assessment (e.g. summary reports) to help you make your decision.

For more information on our CSP IT Security Assessment Program, see *ITSM.50.100 Cloud Service Provider Information Technology Security Assessment Process*.

## TIPS FOR IMPLEMENTING CLOUD SERVICES

Organizations need to adopt a structured approach for managing risks. This approach should account for the use of cloud services to support your organization's goals and outcomes.

Before committing to a cloud-based service, your organization should consider the following tips:

- Review all the existing investments that you have in software, the costs associated with operating on-premises services (e.g. data centers, hardware, networks, talent), and the value that can be gained from having access to new features and functionalities provided by cloud services.
- Identify the value and the level of sensitivity of your information; this exercise will help you identify the information that you can store in the cloud (e.g. low sensitivity information) and will ensure you are adequately protecting sensitive business information and personal information.
- Review the security work that we have already conducted, such as our summary reports on CSPs to find out more about a specific CSP's security controls and processes.
- Ask a CSP to provide security certifications and attestations from third-party auditors so that you have evidence that the provider has a security posture that meets your organization's requirements.
- Use service level agreements to define roles and responsibilities, document requirements for a CSP's performance, and outline financial penalties for underperformance.
- Review and manage security controls that protect the assets that you have in a cloud service, such as web application gateways, network security groups, and security control baselines.

## DATA RESIDENCY CONSIDERATIONS

Data residency refers to the geographical location where data is stored. Your organization may specify a location based on its regulatory and policy requirements.

Data residency is particularly important when it comes to personal information. Different countries may have different requirements for protecting the privacy of personal information. Your organization is responsible for ensuring that the CSP adheres to data residency requirements.

If your organization is a Government of Canada (GC) department or agency, you are required by the Treasury Board of Canada Secretariat to store sensitive GC data within the geographical boundaries of Canada. For non-GC organizations, we recommend that you ensure all sensitive data, including account and security information, is stored within Canada.

## MORE RESOURCES

We have various publications on cloud security that are available on our website, including the following:

- *ITSM.50.062 Cloud Security Risk Management*
- *ITSM.50.100 Cloud Service Provider Information Technology Security Assessment Process*
- *ITSAP.50.110 What is Cloud Computing?*
- *ITSAP.50.111 Models of Cloud Computing*
- *ITSAP.50.112 Steps to Address Data Spillage in the Cloud*

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Visit the Cyber Centre website at **cyber.gc.ca**.