Communications Security Establishment Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Managing the risks to Government of Canada data when using cloud services

MANAGEMENT

Foreword

ITSM.50.109 Managing the risks to Government of Canada Data When Using Cloud Services is an unclassified publication issued under the authority of the Head of the Cyber Centre.

Effective Date

This publication takes effect on August 3, 2022.

Revision History

Revision	Amendments	Date
1	First release.	August 3 2022

D97-4/50-109-2022E-PDF
978-0-660-44634-9

Overview

This document includes guidance to help Government of Canada (GC) departments and agencies manage the risks to GC data when using cloud services, specifically public cloud deployment models.

This document defines GC data and illustrates that a subset of this data can be represented by a cloud service provider's (CSP) terminology and accessed and processed by the cloud service provider's platform for various purposes. It is important for GC departments to recognize what GC data is and understand what this subset of the data can be with services they procure. They should understand the injury levels with sensitive data and the departmental risk of activities. Departments will be able to risk-manage their data and make risk-based decisions when adopting public cloud services to fulfill mission requirements.

This document refers to National Institute of Standards and Technology (NIST) Special Publication 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices [1][1].

[1] Numbers in square brackets refer to resources cited in the Supporting Content section of this document.

Table of Contents

List of tables

1 Introduction

This document offers information on risk management with Government of Canada data when using cloud services. Organizations need to consider risk management in changes where organizations traditionally managed their own data internally to now using external cloud services to manage their data.

When using CSPs to manage information, organizations should consider the traditional internal risks as well as new external threats. This document offers organizations guidance on different information types that need to be evaluated before and while using CSPs to determine the risks involved with that information being stored and handled externally.

1.1 Information types to consider

Before using cloud services, organizations operated their own information technology (IT) infrastructures with personnel who were cleared under the organizations' personnel security requirements. The personnel procured the needed IT equipment, installed them in the data centre, and maintained and managed them to fulfill operational requirements and support mission operations. Organizations maintained controls over the information and the information assets. Identifying all the information types in a traditional IT environment is a complex exercise. Examples of this include:

- Mission data and user data that reside in corporate applications;
- Configuration data that allows applications to function as intended; and
- Application metadata that personnel use to operate and maintain the applications.

Additionally, there is the data concerning the infrastructure that is comprised of endpoints, appliances, servers and network elements, various types of operating systems and firmware, etc. – the data that not only describes what components of the IT infrastructure do, but also their behaviours and how well they function.

The information in an IT system can be viewed from numerous perspectives, such as business domain, architecture, web, database tiers, networking, and others. Each perspective offers specific objectives.

All this data is important. It represents the information held in an organization's IT infrastructure and provides information about the environment. When data is under threat, there are risks to the confidentiality, integrity, and availability of an organization's critical business activities that support mission objectives. Mission operations may not be able to operate correctly or at all, which adversely affects the ability of the organization to deliver products and services. Organizations should account for this data and examine the sensitivity from an operational security (OPSEC) perspective. Many organizations understand the importance and the implications when there is unauthorized access to these data. They understand that they need to account for this data from the risk management perspective and implement necessary policies, standards, procedures, and guidelines to a varying degree to prevent unauthorized access to the infrastructure and guard the information.

This reference to the on-premises IT environment provides a good indication on what a fulsome assessment of GC data should encompass. The GC data can be defined with the following three categories:

1. Data that is related to and supports your organization's mission and goals;
2. Data that describes the supporting IT infrastructure; and

3. Data that enables your organization to operate its IT infrastructures and supports the ongoing function of these infrastructures to meet organizational goals.

The data that users create and operate to support and meet organizational goals, this is the mission-related data that organizations' users can see, access, and process on a daily basis. For illustration of this category of data, the NIST publication SP 800-60 Vol. 2 Rev. 1 [1] has identified a comprehensive list of information types that would cover many aspects of a functional organization, and that can be viewed as various types of business-related data that are created by organizational users to support mission operations.

The other two broad categories of data concerning the IT infrastructure can also be better represented by using information types identified in the NIST publication SP 800-60 Vol. 2 Rev. 1 [1]. The table below describes the information types that are associated with an IT infrastructure.

Table 1: Information and technology management information types

Information Type	NIST 800-60 Definition
System development	System development supports all activities associated with the in-house design and development of software applications.
Lifecycle or change management	Lifecycle or change management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures.
System maintenance	System maintenance supports all activities associated with the maintenance of in-house designed software applications.
IT infrastructure maintenance	IT infrastructure maintenance involves the planning, design, implementation, and maintenance of an IT infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, network access rules, implementing files, switch setting, hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and processes.
Information system security	Information system security involves all functions pertaining to the securing of federal data and systems through the creation and definition of security policies, procedures, and controls covering such services as identification, authentication, and non-repudiation.
Information Management (IM)	IM involves the coordination of information collection, storage, dissemination, and destruction as well as managing the policies, guidelines, and standards regarding IM.
System and network monitoring	System and network monitoring supports all activities related to the real-time monitoring of systems and networks for optimal performance. System and network monitoring describe the use of tools and observation to determine the performance and status of information systems and is closely tied to other IT management sub-functions. System and network monitoring information type should be considered broadly to include an agency's network (e.g. performance, health, and status) and security operations (e.g. intrusion monitoring, auditing, etc.) support.

2 GC data represented in cloud provider terminology

As organizations move into the cloud environment and take advantage of the benefits offered by cloud services, they need to understand what GC data entails, and reevaluate their data in the cloud context. Information types identified in the table above provide information on what components and configurations are contained in a particular IT environment – what they do and how they function, as well as how well the IT infrastructure operates – where strengths and vulnerabilities can be identified or inferred. In a cloud environment, some of the data in each information type can no longer be viewed as completely under an organization's control. Organizations can still access, process, and manipulate this data, however, so can service providers for the purposes of operating and maintaining the service performance and security of their platforms. Organizations need to understand how service providers describe this information to have an objective dialogue and make an informed and risk-based decision.

2.1 User data or customer data

Mission-related, or business data, is the data that users of an organization either create or upload into mission applications and that users need to process to support mission operations. In the cloud environment, this data is the information that users enter and create within procured cloud services. It is typically described by the CSP as user data or customer data. The providers develop comprehensive data security and data privacy policies to be compliant with various laws and acts in many jurisdictions to ensure that this type of data is protected from both the security and privacy perspectives. For example, ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information [2] specifies cipher suites to be used for data encryption; while the *Privacy Act and Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use, and disclosure of personal information. Some provinces have also enacted their own version of privacy laws for their respective jurisdictions.

Even though there are strict rules governing the access and the processing of the user data by the providers, organizations should always be prudent about their user and business data and understand the circumstances where their data may flow and be stored in different jurisdictions. This creates a scenario for organizations to question whether measures that service providers have put into place can be considered sufficient. For example, providers may need to access and process copies of user data to both ensure the service performance and assist customers in resolving specific issues. In these cases, user data must be free of personal identifiers so that the information cannot be attributed to any specific individual.

2.2 Data that contains IT infrastructure information

Evaluating the impact caused by compromise of the data that contains IT infrastructure information is not as intuitive as that of user data. It is not a topic that one encounters when discussing organizational data types. It is almost certain that when organizations bring up the topic of data in the public cloud context, that the discussion would naturally turn into a user data discussion. This may be due to:

1. The IT infrastructure data is not as visible as user data in terms of direct contribution to mission operations; or
2. The organization places less emphasis on the IT infrastructure data ownership in the public CSP due to a lack of control and awareness.

Each organization needs to understand their perspective on the issue of data types and the relationship with their CSP. Organizations need to consider all data types in the same way they manage data in their on-premises IT environment. Different areas organizations should consider when using cloud services include:

- Identifying the responsibilities for the providers and the customers in the cloud service model;
- Understanding the need to perform their responsibilities to secure and risk manage their data and cloud environment;
- Communicating with the CSP on their service model to identify data ownership and data access.
- Discussing with the CSP on what kind of analytics are processed and whose analytics process the data.

When organizations stand up their cloud environment, they may have hundreds or thousands of workloads (i.e. a complex environments), whereas others may simply deploy a few applications. The cloud infrastructure that underpins these environments is similar in nature and all of them should have sound and securely configured networking services, computing services, storage services, and management services. The difference among organizations' cloud environments is the way individual organizations set up and configure the services to behave and function in a manner that is specific to the mission. There are many types of data, such as various types of configurations, performance monitoring information, security monitoring information, and access control information, that could shed light on IT infrastructure in a government system. This information, along with configured services, are the essential parts of a functional cloud environment where the organization owns, accesses, processes and analyzes the information themselves. Equipped with this information and the configured services, organizations have a functional cloud environment. They own, access, process, and analyze the data and the information. However, in public cloud offerings, some of this data can also be accessed and operated by the cloud service providers.

The CSPs, in many cases, must have access to this data that contains information on organizations' cloud environments to fulfill their service level agreements. For example, the CSPs need to manage service performance, service customization, security of their platforms, and service offerings. It is necessary to understand how the organization's cloud infrastructure data and information is represented under the CSPs' terminology. This understanding allows organizations to have a meaningful discussion with the providers to cover the necessary security considerations to ensure the data is secure and protected from unauthorized access and modification. For example, a service's data plan is in a jurisdiction that meets the customer's compliance and policies requirements, but the service's management plan may reside in a different jurisdiction. If this is a concern, the organization needs to understand what data or subset of data provides infrastructure data that can be accessible by the management plan and what other processing activities there might be. There should be a collaborative dialogue between the organization and CSPs. It is useful to recognize the terminology used by the providers that could contain the organization's data or the representation of organization's data. Table 2 outlines some of these examples.

Table 2: GC data represented in cloud terminology

Data Type	Definition
Customer and user data	Data, including text, sound, video or image files, and software that customer provides to CSP. This includes data customers upload for storage or processing and apps that customers upload for distribution.
Object metadata	Data generated during the service runtime. Can include information provided by the customer, or on the customer's behalf, that is used to identify or configure service resources (i.e. software and systems). Some examples of this information include: names and technical settings of storage accounts, virtual machines, databases, and data collections (e.g. tables, column headings, labels, and document paths). Metadata that may be shared across CSP's global infrastructure to facilitate operations and troubleshooting
Service generated metadata	Data generated and derived by a service provider through the operation of a cloud service. Service provider groups this type of data together to ensure performance and security.
Diagnostic data	Telemetry data and data obtained from applications that customers install locally to use when connecting to cloud services.
Access control metadata	Data used to manage access to other types of data or functions within services.

3 Security categorization of data

Understanding that the data types used by CSPs can manage sensitive information, organization's need to perform risk management analyses to understand the potential injury of the data and make informed risk-based decisions.

Security categorization is one of the fundamental steps of the cloud security risk management approach, as defined in ITSM.50.062 Cloud Security Risk Management [3]. Security categorization is the process of identifying the potential injuries that could result from compromises to business processes, business activities, and related information. To categorize business processes and activities, one must first determine the expected injuries that could result from a compromise and the level of these expected injuries.

The NIST publication [1] has suggested a baseline security categorization for the IT infrastructure information types. Table 3 leverages the recommendation from NIST and maps GC information types to data types described in cloud terminology. This table recommends baseline security categorization of the mapped data types in the Protected B, medium integrity, and medium availability (PBMM) context.

Table 3: Security categorization for general purpose GC domain (PBMM profile)

Information Type	Mapped CSP Data Type	Security Categorization		
		Confidentiality	Integrity	Availability
Mission-related information	Customer data	Medium	Medium	Medium
System development information	Customer data	Low	Medium	Low
Lifecycle and change management information	Customer data	Low	Medium	Low
System maintenance information	Service-generated data	Low	Medium	Low
IT infrastructure maintenance information	Object metadata Access control metadata	Medium	Medium	Medium
Information system security information	Customer data	Medium	Medium	Medium
Information management information	Object metadata	Low	Medium	Low
System and network monitoring information	Service-generated data Object metadata Diagnostic data	Medium	Medium	Medium

The injury levels defined in the table should be considered as a baseline or a minimum injury level in the PBMM context. Organizations are strongly recommended to take their respective business activities and nature of mission sensitivity and criticality into consideration. They may arrive with higher injury levels for certain data types with respect to the confidentiality, integrity, and availability of security objectives and should be considered in the cloud risk management approach [3].

Another factor that should be considered is when the data or subset of the data that is stored, processed, or both in jurisdictions outside of Canada. Data types identified above may be moved to other jurisdictions for storage or processing depending on the CSP’s platform architecture. CSPs that operate in other jurisdictions are subject to local laws with which they need to be compliant. There can be integrity and availability implications on organization’s mission operations. Information that resides in other jurisdictions could be subject to foreign laws that could disclose GC data.

4 Summary

While mission-related data types are important, organizations cannot overlook the importance of data types that provide information and insight of their IT environment. These important data types are protected when operations reside on-premises. Stronger security considerations should be taken into account for IT infrastructure data types when moving into the public commercial cloud environment. Organizations should engage with CSPs to understand possible differentiating terminology, how your data is represented, where the data is located in the CSP’s infrastructure, and assess data injury levels by performing a security categorization analysis [3]. They should feed the analysis into a risk management process to ensure informed and risk-based decisions are made by accounting for all the data.

5 Supporting content

5.1 List of abbreviations

Term	Definition
CSE	Communications Security Establishment
CSP	Cloud service provider
GC	Government of Canada
IM	Information management
IT	Information technology
ITS	Information technology security
OPSEC	Operational security
PBMM	Protected B, medium integrity, and medium availability
PIPEDA	*Personal Information Protection and Electronic Documents Act*

5.2 Glossary

Term	Definition
Access control	Certifying that only authorized access is given to assets (both physical and electronic). For physical assets, access control may be required for a facility or restricted area (e.g. screening visitors and materials at entry points, escorting visitors). For IT assets, access controls may be required for networks, systems, and information (e.g. restricting users on specific systems, limiting account privileges).
Authentication	A process or measure used to verify a users identity.
Authorization	Access privileges granted to a user, program, or process.
Cloud service provider	Any commercial provider that offers cloud computing services to provide on-demand availability of computer system resources.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Encryption	Converting information from one form to another to hide its content and prevent unauthorized access.
Injury	The damage to the national interests and non-national interests that business activities serve resulting from the compromise of IT assets.
Injury level	The severity of an injury, which is defined in five levels: very low, low, medium, high, very high.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it’s not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Operational security control	A security control primarily implemented and executed by people and typically supported by the use of technology (e.g. supporting software).
Risk level	In the cyber security context, the likelihood and the impact of a threat using a vulnerability to access an asset.

Term	Definition
Threat	Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information.

5.3 References

Number	Reference
1	National Institute of Standards and Technology (NIST) *Special Publication 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008.
2	*ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information*, August 2016.
3	*ITSM.50.062 Cloud Security Risk Management*, March 2019.