Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR
CYBER SECURITY

Recommended cyber security contract clauses for cloud services

Management

TLP:CLEAR

Canada

Foreword

This is an UNCLASSIFIED publication, issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our Contact Centre at:

contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on October 22, 2024.

Revision history

Revision	Amendments	Date
1	First release	October 22, 2024

ISBN 978-0-660-73402-6
CAT D96-123/2024E-PDF

Overview

As more organizations move to cloud-based services and technologies, there is a growing need to identify supporting contract clauses and principles to ensure cyber security expectations are clearly understood and documented. Cyber security clauses and principles are important service components. They should be combined with foundational contract elements, such as service level agreements (SLAs), task orders, and governing standards.

When combined, these contract elements and clauses provide a service framework to ensure your organization receives the services and solutions you expect and provide proper assurance that their data and identities are secure.

This publication outlines common areas for cloud service contracts and procurement from a cyber security perspective for both government and non-government organizations The recommendations provided should be considered along with the main functional and legal aspects of service contracting when working with any cloud service provider (CSP).

Table of contents

List of figures

1 Introduction

The guidance in this publication highlights important security considerations for your organization as you develop and review your cloud service contractual requirements with cloud service providers (CSPs). Your organization should manage the associated risks when contracting and relying on cloud services for your critical business processes. There can be gaps in the contract provisions if the cyber security components in a cloud service procurement model are managed through traditional means. These gaps can leave your organization unable to manage the complexities associated with modern cyber security services.

While CSPs may present initial foundational service conditions and terms, your organization's management team is responsible for demonstrating and validating that the terms and conditions of the contract address your organization's business security needs. The terms and conditions should be adaptable for future modifications to safeguard the interest of your organization. The terms and conditions in the service contract should also provide your organization with the best possible business outcomes. Your organization must initiate proactive measures to ensure service provisions include cyber security mechanisms for identifying, communicating, mitigating, and preventing risks.

This publication outlines common cyber security considerations for assessing cloud service contracts and procurement risks. It is recommended that these be considered along with the main functional and legal aspects of contracting when working with a CSP. These areas of consideration should also be applied when engaging other service providers such as a managed service provider (MSP), a managed security service provider (MSSP), service integrator (SI), or service orchestrator (SO).

The clauses outlined in this publication are not to be considered legal advice. Rather, they offer context for your organization when considering cloud services and you are presented with terms and conditions from the potential service provider. This guidance can assist your organization in knowing what to consider or what questions to ask when moving to the cloud.

1.1 Scope

This publication provides advice and guidance in the areas of cloud service contracting. In all cases, application of this guidance can fall both on your organization as the consumer, as well as on the service provider. The examples listed are not meant to be an exhaustive indication of best practice but do offer insight into clauses that have been used successfully by government and industry partners.

Disclaimer: The Communications Security Establishment and the Cyber Centre do not recommend or endorse the use of any particular contracting clause listed in this document. Information provided is only intended to be a source of examples of contract clauses that may be useful for cloud service contracting and is provided for informational purposes only.

1.2 Guiding documents

In preparing this guidance, we have considered inputs from various reference documents and frameworks.

1.2.1 Government resources

The following list provides references to related policies and guidance documents that were considered in the development of this publication:

- IT Security Risk Management: A Lifecycle Approach (ITSG-33) [1]
- Technology Supply Chain Guidelines (TSCG-01) [2]
- PSPC Contract Security Manual [3]
- FedRAMP Control – Specific Contract Clauses version 3.0 [4]
- NIST SP 800-171 - Enhanced Security Requirements for Protecting Controlled Unclassified Information [5]
- NIST SP 800-172- Enhanced Security Requirements for Protecting Controlled Unclassified Information: Supplementary [6]

1.2.2 Industry resources

Additionally, we have considered the following industry standards and frameworks:

- ISO 27001:2022 – Information Security Management Systems [7]
- ISO 27017:2015 – Guidelines for Information Security Controls [8]
- ISO 27018:2019 – Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds as PII Processor [9]
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing [10]

1.2.3 Recommended nomenclature

All resources indicated above provide various levels of detail and technical nomenclature in relation to cloud services. From a strictly contract perspective there are terms that will assist you in procuring cloud services based on “point in time” or “future need”. Section 2.1 lists the various forms of intention that your organization will need to consider based on the cloud services required. In some cases, your organization may need to be aware that some cloud services may need time to re-engineer or may have updated features in a roadmap. Your organization should consider your immediate needs and those that can be developed in stages or at a later time.

Your organization should establish the mandatory and rated requirements your organization needs. Mandatory requirements are those that the provider ”must” have or ”shall” provide. When looking to rated requirements, your organization can look to the use of ”should”, “may”, or “consider” provisioning. These areas would also denote that the provider already has these elements in place. In those cases where services are on a roadmap or not yet in place, your organization will need to look for terms such as “will” or “capable of achieving” to indicate the future expectation.

2 General cyber security considerations

In order to establish security expectations within enterprise cloud service contracts, the selected service model construct influences the choice of security services available. Understanding the shared responsibility model can provide clarity and information on security control options accessible to consumer organizations. For example, the management of access control mechanisms relies on the customer to implement and deploy system control functions as much as it depends on the CSP to provide the underlying supporting infrastructure. These interactions are established within logical security, hardware and physical security, personnel security, and information technology (IT) security domains. These areas are then further defined utilizing specific contract language and references to a requisite security controls profile or overlay. Typically, references to ITSG-33 [1], NIST 800-53 Security and Privacy Controls for Information Systems and Organizations [10], and other variants provide security control catalogues and references or suggestions to specific "security profiles." The goal is to reduce the probability for risk events and reduce uncertainty with well-defined requirements in the overall management of the contract.

2.1 Main considerations

There are several main areas your organization should focus on when reviewing cloud service models. Each area is incorporated into specific contract clause language. However, they are offered here as a point of consideration when looking at how to categorize and to determine what types of cloud services are required. The initial areas of consideration are:

- assessment
- incident management
- key management
- endpoint protection
- remote management
- privileged access management
- cryptographic assurance
- data protection
- identity and access management
- secure development
- security testing and validation
- network and communications security
- federation
- information spillage
- logging and auditing
- continuous monitoring
- data sovereignty

- data residency

For further information on categorization and classification of service models, we recommend reviewing the Cyber Centre's Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103) [11].

2.1.1 Data security and protection

Data security represents a core service expectation within the cloud service model. To ensure maximum effectiveness of data security controls, your organization should implement a layered service approach. Service contracts should define CSP responsibilities on your data and their limitations with respect to intellectual property rights on your organizational data, inferred data, or constructed data. Contractual agreements should differentiate between data at rest, data in transit, processing, and storage. Security requirements around encryption protections, approved geographical repositories, limitations on transit flows, and access control measures should be documented. Mitigation measures implemented to reduce or eliminate risks associated with data retrieval and destruction processes should be documented as well. You should review data residency policies and service choices as they relate to your specific business regulatory environment. Some services and data centres may not reside in Canada which can have an impact on your organization's ability to protect data in accordance with legislative or regulatory requirements.

Risks associated with emerging technologies are also a growing concern. You should consider limiting the impact of such technologies, like artificial intelligence (AI), machine learning, and quantum computing on your data. Address potential risks through proactive contract clauses that mandate specific procedures, exclusions, or restraints to be followed when using your data.

Example clause structure and language

The contractor must:

- Implement encryption of data at rest for the cloud services hosting the organization's data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with cryptographic protection recommended by the Cyber Centre in Guidance on Cloud Service Cryptography (ITSP.50.106) [12] .
- Transmit the organization's data in a secure manner providing the ability for the organization to implement encryption for data in transit for all transmissions of its data, in accordance with cryptographic protection and network and communications security as recommended by the Cyber Centre.
- Take appropriate measures to ensure that its personnel do not have standing or ongoing access rights to the organization's data and that access is restricted to CSP personnel with a need-to-know, including resources that provide technical or customer support, based on appropriate approval.
- Report intended or accidental violations to data protection and cryptographic mechanisms to the customer organization, providing documentation and evidence on planned action or action taken to redress the situation.
- Support cryptographic agility such that the protection of data in transit or at rest can remain current with cryptographic protection recommendations from CSE and the Cyber Centre, including the use of new standards to mitigate the quantum computing threat. For more information, see Guidance on Becoming Cryptographically Agile (ITSAP.40.018) [13].

References

- GC Cloud Guardrails – Protection of data-at-rest [14]
- GC Cloud Guardrails – Protection of data-in-transit [15]

2.1.2 Data residency and sovereignty

Contractual clauses specifying data sovereignty and residency requirements should be documented for all forms of data and cloud services within required regulatory environments. Contracts should mandate the CSP to inform the customer in scenarios where organizational data is moved to an unapproved region. Data outflows from cloud platforms are often designed to be expensive, while incentives exist to facilitate data inflows to a CSP's platform. Avoid contractual models which expose your organization to lock-in risks and design agreements which guarantee access to your organization's data within a reasonable cost structure.

The contractor must store and protect your organization's data, at rest, including data in backups or maintained for redundancy purposes. This includes the ability to isolate data in Canada in approved data centres. An approved data centre should:

- meet specific security requirements and certifications identified by your organization's regulatory requirements
- ensure that a specific customer's data cannot be found on physical media
- employ encryption to ensure that no data is written to disk in an unencrypted form, in accordance with cryptographic protection as recommended by the Cyber Centre

Example clause structure and language

The contractor must:

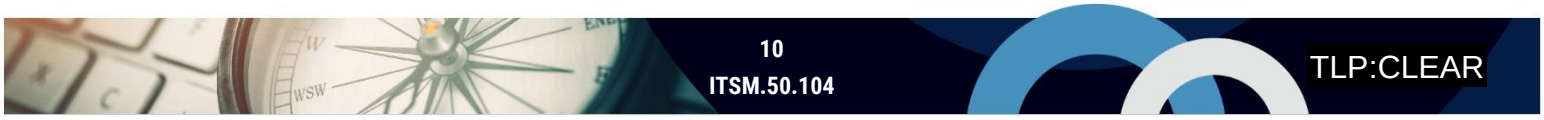
- Take appropriate measures to prevent the transmission of organizational data outside of agreed service and geographical regions except when organizational approval is received.
- Provide the capability and tools to extract all information including, system configurations, activity logs, and object and file storage information such that the organization can validate the location and activity record for its data.

References

- GC Cloud Guardrails – Data location [16]
- Guidance on cloud security assessment and authorization (ITSP.50.105) [17]

2.1.3 Supply chain integrity (SCI)

Supply chain risks pertain to the activities of threat actors to exploit supply chain vulnerabilities in an effort to compromise the integrity of one or more system components to achieve their broad objectives. For organizations to protect against such threats, contractual agreements must consider supply chain security, to the extent or capability of the organization, including threats from points of manufacturing, transportation, integration, and operation. As part of the cloud service procurement process, your organization should conduct supply chain risk assessments and request that CSPs provide information on their supply chain risk management plans, ownership information, subsidiary relationships, and third-party relationships.



Should there be a concern with the release of such information or indication as to who the CSP's suppliers are, discussions on third-party assurance through a mutually agreed entity is recommended. Your organization can also consider using the Cyber Centre's Harmonized Threat Risk Assessments (HTRA) [18] methodology or the Analytical Software for Threat Assessment (ASTRA) tool to conduct threat risk assessments (TRA) and evaluate potential risks associated with their projects.

Example clause structure and language

The contractor must agree to:

- Provide information required for the customer to conduct a supply chain security assessment, including information on ownership structure, corporate registration, investors and management executives, suppliers, sub-contractors, sub-processors, third-party relationships, and any other information required for such assessment.
- Support the supply chain security assessment by providing information related to equipment, firmware, software, or any other systems as required.
- Maintain a supply chain risk management (SCRM) plan that describes the CSP's approach to SCRM and demonstrates how the contractor's approach will reduce and mitigate supply chain risks.
- Implement and maintain safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide services.

References

- Cyber supply chain: An approach to assessing risk (ITSAP.10.070) [19]
- Supply chain threats and commercial espionage [20]
- Contracting clauses for telecommunications equipment and services (TSCG-01L) [21]
- ISO/IEC 27036 – Cyber security – Supplier relationships (Parts 1 to 4) [22]

2.1.4 Identity and access management, privileged access, and federation

Cloud-based identity and access management (IAM) models expose unique security challenges due to their shared responsibility service structure. How user accounts, system services and entities are identified, authenticated, and how their permission rights are managed may require coordination of multiple partners (customer, CSP and identity provider (IDP)). Contract clauses used to manage services should clearly delineate account management responsibilities for all parties. Service contracts should document mitigations against unauthorized non-privileged or privileged user or system access. Federation of identities and credentials should be restricted to within agreed trust frameworks. Unauthorized third-party access (user or system) to your organization's data or cloud instance should be restricted. Service agreements should mandate access logging, and retention periods should be sufficient to facilitate audit and incident response activities. Service contracts should address CSP obligations with respect to application backdoors or unauthorized system-based access (APIs).

Example clause structure and language

Identity and access management

The contractor must provide the ability for your organization to support secure access to cloud services including, but not limited to configuring:

- phishing-resistant multi-factor authentication (MFA) in accordance with User Authentication Guidance for Information Technology Systems (ITSP.30.031) [23] using GC-approved credentials
- role-based and behaviour-based access
- access controls on objects in storage
- granular authorization policies to allow or limit access

The contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

Privileged access management

The contractor shall make use of secure and trusted endpoint devices to perform its system administration functions such as a dedicated administrative privileges workstation designed with restricted configurations, system functionality, and security controls.

Federation

The contractor shall ensure that federation of authentication mechanisms, including corporate identity and attribute information are protected in accordance with the current NIST Digital Identity Standard NIST SP 800-63-4 Digital Identity Guidelines: Federation and Assertions [25] or the Cyber Centre's ITSP.30.031 [23].

References

- Top 10 IT Security Actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) [24]
- Digital Identity Guidelines – NIST Special Publication 800-63-4 [25]

2.1.5 Incident response and management

Contractual clauses managing incident response activities must implement a risk-based approach. They must consider potential service outages and expected service recovery targets, especially as they impact industry regulations and reporting requirements. Your organization should consider clauses mandating incident information disclosure to assist with assessing the impact, severity, and materiality of an incident which may require regulatory notification and oversight. Some examples of these types of clauses can include:

- notifications when a service is affected
- disclosure of any known vulnerabilities and associated patches
- provision of log information to an entities SOC team for ingestion

Additional features or the disclosure of specific information on the service is a consideration for your organization's security and monitoring needs and capabilities.

Regulated entities, as well as critical infrastructure organizations offering services supporting critical national services, with impact on national security or public safety may require additional oversight. A service disruption can have wider national security and human safety implications. Effective incident response capabilities require coordination among many internal and external entities. Your contractual agreements must clearly define responsibilities for all stakeholders.

Example clause structure and language

The contractor must:

- Establish and maintain a security operations centre (SOC) capability that operates within your organization's defined time of operation and service model, such as 24/7 service coverage.
- Establish and maintain a cyber incident response team that can be deployed by the CSP within your organization's expected service targets.

References

- Managing the risks to Government of Canada data when using cloud services (ITSM.50.109) [26]
- Guidance on defence in depth for cloud-based services (ITSP.50.104) [27]

2.1.6 Cryptographic assurance and key management

Access to sensitive cryptographic materials and keys should be restricted. Secrets such as cryptographic keys, database credentials, APIs, and certificates represent sensitive components that require extensive oversight. The lifecycle of these components and how they are managed and deployed should be captured in the service contracts. Cryptographic processes should use the latest FIPS-validated or Cyber Centre-approved cryptographic algorithms. The security of a CSP's master keys also impacts the safety of organization-specific keys linked to your services.

Example clause structure and language

The contractor must:

- Ensure that cryptographic operations and the protection of critical security parameters (e.g. cryptographic keys) are performed in cryptographic modules certified by the Cryptographic Module Validation Program (CMVP). The cryptographic module should be configured and operated in an approved mode in accordance with the CMVP-published security policy.
- Ensure that the CSP master key or root keys used for deriving other keys are generated and managed through secure and approved FIPS 140-validated processes for key generation, distribution, storage, and lifecycle management.

References

- Guidance on cloud service cryptography (ITSP.50.106) [28]
- Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111) [29]

2.1.7 Endpoint devices and media security

The resilience of the cloud infrastructure is dependent on the reliability of device components and associated software services. Where possible, service contracts should address the resilience of device components supporting critical service functions. Service agreements should address the reliability, resilience, performance, and operational targets on hardware and software components. Agreements should address access restrictions to removeable media, destruction procedures, media transport, and distribution limitations.

Example clause structure and language

The contractor must:

- Implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks, and misuse in accordance with industry-recognized configuration guidelines such as those found in NIST 800-123 Guide to General Server Security [30], the Center for Internet Security (CIS) benchmarks [31], or an equivalent standard approved by the organization in writing.
- Securely erase, purge, dispose, or destroy resources, such as equipment, data storage, files, and memory or devices that may contain your organization's data and ensure that previously stored data cannot be re-instantiated from systems or devices.
- Design and implement operational measures to ensure software, hardware and network communications systems support redundant and resilient services to withstand disruptions, hardware failures, and destructive cyber events.
- Ensure digital and non-digital media containing organizational data is protected by cryptographic mechanisms to protect the confidentiality and integrity of this information.

References

- Securely configure devices [32]
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) [33]
- Secure your devices, computers, and networks (ITSAP.00.007) [34]
- Using your mobile device securely (ITSAP.00.001) [35]
- How updates secure your device (ITSAP.10.096) [36]

2.1.8 Network and communications security

Communication systems (wireless or wired) extend the capability of cloud platforms to process data and provide on-demand network and computing resources. As data moves from one point to the other, network paths, network devices, the control plane, and interconnectivity with other services require protections against vulnerabilities and cyber attacks. Cloud computing platforms require trusted network components, secure communication paths, and governance models to deliver trusted services. Customer organizations must ensure trusted communication system requirements are included in service arrangements with CSPs.

Example clause structure and language

The contractor must:

- Provide the capability to establish secure connections to its platform, including protecting the confidentiality, integrity, and availability, such as using Transport Layer Security (TLS) for data-in-transit encryption and mutual TLS support to verify the identity of clients and services.
- Provide the ability for your organization to implement dedicated or private connections to its data centres and support for sensitive workloads that may require such connections.
- Provide tools and capabilities to assess the effectiveness of security controls and provide visibility into the enforcement of security controls across the data transit path using technologies such as activity logs and reporting.
- Validate the security posture and uniquely identify and authenticate requests before establishing a network connection to the customer organization's tenant or cloud resources.

References

- Cloud network security zones (ITSP.80.023) [37]
- Guidance on securely configuring network protocols (ITSP.40.062) [38]
- Guidance on cloud security assessment and authorization (ITSP.50.105) [17]

2.1.9 Continuous monitoring

Continuous monitoring of the state and security of the cloud service is essential. Managing logs, monitoring network traffic, and monitoring application service components are just a few of the related activities. Activity logs, system logs, audit logs, and events logs are examples of crucial components required for conducting monitoring and analytics to assess and validate in the cloud. Monitoring performance metrics should also be included as part of the periodic reporting capabilities.

Example clause structure and language

The contractor must:

- Actively and continuously monitor threats and vulnerabilities to cloud service infrastructure, applications and services and, your organization's data.
- Conduct regular vulnerability scans and penetration testing of the contractor infrastructure and service locations, with the aim of identifying deficiencies and remediations to prevent unauthorized access to sensitive information, circumvention of access controls and privilege escalation, and exploitation of vulnerabilities to gain access to systems or information.
- Log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, and (vi) deletion of data.
- Implement protections to prevent service exhaustion attacks through security measures such as denial of service protections.

References

- Network security logging and monitoring (ITSAP.80.085) [39]
- Cyber security considerations for consumers of managed services (ITSM.50.030) [40]

2.1.10 Secure development, testing, and validation

The management of the software and system development lifecycle affects several cloud service components. The service contract must establish or describe secure management of software lifecycle, including the management of vulnerabilities, patch management cycle, and open-source software security.

Example clause structure and language

The contractor must:

- Provide relevant information on known security vulnerabilities relating to systems owned or controlled that may require your organization's action to successfully resolve or protect against such vulnerability.
- Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the cloud services or libraries used by the cloud services and provide advance notices of patches in accordance with agreed upon service-level commitments.

References

- Top 10 IT security action items: No.2 patch operating systems and applications (ITSM.10.096) [41]
- Automatically patch operating systems and applications [42]

2.2 Complimentary considerations

Complimentary considerations serve as additional cloud service baseline requirements and supporting security principles.

2.2.1 Privacy risks

Your organization may have concerns about the potential impact on privacy and risks related to breaches of organizational data in the cloud. You should consider the privacy issues and the impact on the security of your organization's data. To determine your necessary privacy protections, your organization should review the service provider's management controls (policies and procedures) and technical controls. An independent assessment of privacy controls and their effectiveness should also be considered. Privacy impact assessments should be considered throughout the cloud service lifecycle to ensure related risks are being properly managed.

2.2.2 Personnel security

Your organization should confirm that personnel screening and criminal background checks are being completed for CSP employees as part of your contractual engagement. The CSP should provide evidence of personnel screening policies, security controls, and a compliance regime. Details of the personnel security clearances must be clearly documented, and procedures must be put in place to manage personnel transfer and termination. For employee role transitions, changes to

credentials and authenticators should be executed in a timely manner. Non-disclosure agreements should be in place for CSP employees with access to organizational business data.

2.2.3 Physical security

Due to the nature of the cloud service model, physical security considerations are not often prioritized within service agreements. The security requirements for your organizational data remains the same wherever it may reside (on-premises or in the cloud). Contractual agreements must address physical security requirements to support your assets and data within the CSP's infrastructure. Contractual clauses should emphasize physical restrictions regarding your data and sensitive corporate information.

Data confidentiality security controls, such as encryption or other data transformation mechanisms, do not change the classification of your data. Ensure that your physical security requirements can support all data and assets it handles. Physical access to your organization's data or resources should be restricted to authorized personnel. Contract agreements should address physical security of communications infrastructure, prevention of modification, and tampering of assets. Ensure that security monitoring evaluates the effectiveness of physical security measures and that access logs to physical sites are maintained and audited periodically.

2.2.4 Data retention and destruction

Data retention and destruction security requirements should be defined to ensure the organization, CSP, and other third-party service providers understand their obligations with respect to data retention periods, data handling processes, and destruction processes. Your organization should ensure contractual documents define parameters on acceptable media types, data retention length, media protection controls, sanitization or destruction mechanisms, and destruction verification methods. These parameters should be aligned with the classification of data being protected. Data retention and destruction requirements should apply to all forms of data, including structured and unstructured forms. Periodic assessments should be scheduled to validate that contractual obligations are being met. For more information, see IT Media Sanitization (ITSP.40.006) [43].

2.2.5 Artificial intelligence

Artificial intelligence (AI) and machine learning tools are driving innovative capabilities and altering how system applications and services are delivered. These present unique threats and challenges, particularly with growth in the use of large language models (LLM) and generative AI. Organizations may need to pay attention to the security and privacy implications of AI-based solutions within their value chain. AI is being used to develop new services and these solutions are being trained with business data. Unauthorized AI tools accessing your confidential and operational data presents significant business and privacy risks. Service contracts should address limitations and restrictions related to AI tools accessing your data.

2.2.6 Quantum threat

Cryptography is an effective way to protect the confidentiality and integrity of information and to defend IT systems from cyber threat actors. Quantum computing threatens to break much of the cryptography we currently use. Quantum computers will use quantum physics to efficiently process information and solve problems that are impractical to solve using current

computing capabilities. Quantum computers that are available now are not powerful enough to break cryptography, but the technology is advancing quickly and could be available by the 2030s. However, threat actors can steal encrypted information now and hold on to it until a sufficiently powerful quantum computer is available to decrypt, read, or access the information, even well after the information was created.

To manage the risks associated with quantum computing advancements, your organization should evaluate the sensitivity of the information being shared with your vendor and determine its lifespan to identify information that may be at risk, which can be incorporated as part of your ongoing risk assessment processes. Additionally, your organization should discuss whether the contracting organization has plans to address the quantum threat. Contract agreements should specify that the contractor must keep their cryptographic processes up to date in accordance with the Cyber Centre's guidance Addressing the quantum computing threat to cryptography (ITSE.00.017) [44].

3 Terms and conditions

From a security perspective, contract elements must be prescriptive and conform to recognized frameworks and approaches in order for the CSP to establish how they address and maintain the security posture as indicated by your organization. In many cases, reliance on a given provider's terms and conditions as outlined in a contract or end user licensing agreement (EULA) can be considered as acceptable. However, for some organizations with specific needs or for those that are bound by regulated authorities, negotiation between legal teams using some of the example clauses noted in this guidance may be required. In all cases, where possible seek legal advice if there are any specific areas of concern.

3.1 Considerations

Your organization should consider and discuss the following items with legal counsel and the provider.

3.1.1 Trade secret protections (such as patented material and legal branding)

If your organization has regulatory requirements or has partnerships or joint venture considerations, you should ask how this type of information is separated or further secured within the main tenancy. This will assist you in identifying information that can be easily flagged and separated from general information orders or when a legal hold is indicated. Any terms and conditions must also clearly stipulate that placement of this information within the service provider does not denote a release by your organization to have, hold, or use such information, and that it remains the property of your organization.

3.1.2 Intellectual property

As with trade secrets, intellectual property does not hold official registration like a patent, but it does have direct bearing on your organization's purpose or mandate and will need further measures to tag, identify, and secure. Any terms and conditions must also clearly stipulate that placement of this information within the service provider does not denote a release by your organization to have, hold, or use such information and that it remains the property of your organization.

3.1.3 Indemnification/limitation of liability

In all cases of contracting a certain level of liability is required and must be clearly outlined between parties. Cloud offers a new dynamic in this regard. Attention to how the provider accomplishes "security of the cloud" and describes it within the terms and conditions is very important. It must be noted where the line of responsibility comes into play for "security in the cloud" as this is your organization's responsibility. Depending on whose tenancy is being used, this may become more complex when contracting a managed service provider, service or system integrator, or service orchestrator. A further description of tenancy ownership is detailed in section 3.2.

3.1.4 Support

The model of support can be of interest or concern to regulated organizations. Typically, CSPs are "global" in nature and will indicate that a "follow the sun" approach is used to gain coverage worldwide, 24/7, 365 days a year. This means that all

service coverage is distributed across multiple global locations that cover a specific time zone. For any organization that has regulations as to where support or contracted resources can reside, discussion with the provider is recommended.

3.1.5 Migration

While it is always the intention of an organization to gain a trusted partner, there may come a time when movement of your information to a different provider is considered or possibly necessary. In this matter, initial review and questions regarding migration of information at the outset of the contract would be considered and discussed with the provider. Specific actions to request information on are:

- ingress and egress charges for the movement of data
- time allotments for migration activities once this is indicated to the primary provider
- length of time data is present in the tenancy once information has been migrated

Note: Data sanitization or removal as per the Cyber Centre's guidance IT Media Sanitization (ITSP.40.006) [43] is not applicable within the cloud. Rather, use crypto shredding and provider attestation that indicates to what level of assurance the data is overwritten.

3.2 Tenancy ownership

As mentioned earlier, there are specific distinctions as to who provides or may be responsible for "security of the cloud" and "security in the cloud." There is also the stipulation of where your organization "hosts" your information. This can be done in two specific ways:

- hosting within your own tenancy (owned/controlled)
- being hosted within a provider's tenancy

Your organization must understand the difference between a CSP and an MSP. The main difference is found in the control exerted over the data and process and by whom. In an MSP, the consumer dictates the technology and operating procedures. According to the MSP Alliance, MSPs typically have the following distinguishing characteristics:

- some form of network operation centre (NOC) service
- some form of help desk service
- ability to remotely monitor and manage all or a majority of the objects for the customer
- ability to proactively maintain the objects under management for the customer
- capacity to deliver these solutions with some form of predictable billing model, where the customer knows with great accuracy what their regular IT management expense will be

With a CSP, the service provider dictates both the technology and the operational procedures being made available to the consumer. This means the CSP is offering some or all of the components of cloud computing through a software as a service (SaaS), infrastructure as a service (IaaS), or platform as a service (PaaS) model.[1]

To establish the areas of responsibility more clearly, figure 1 provides a more granular description of the shared responsibility model.

Figure 1: Cloud shared responsibility model

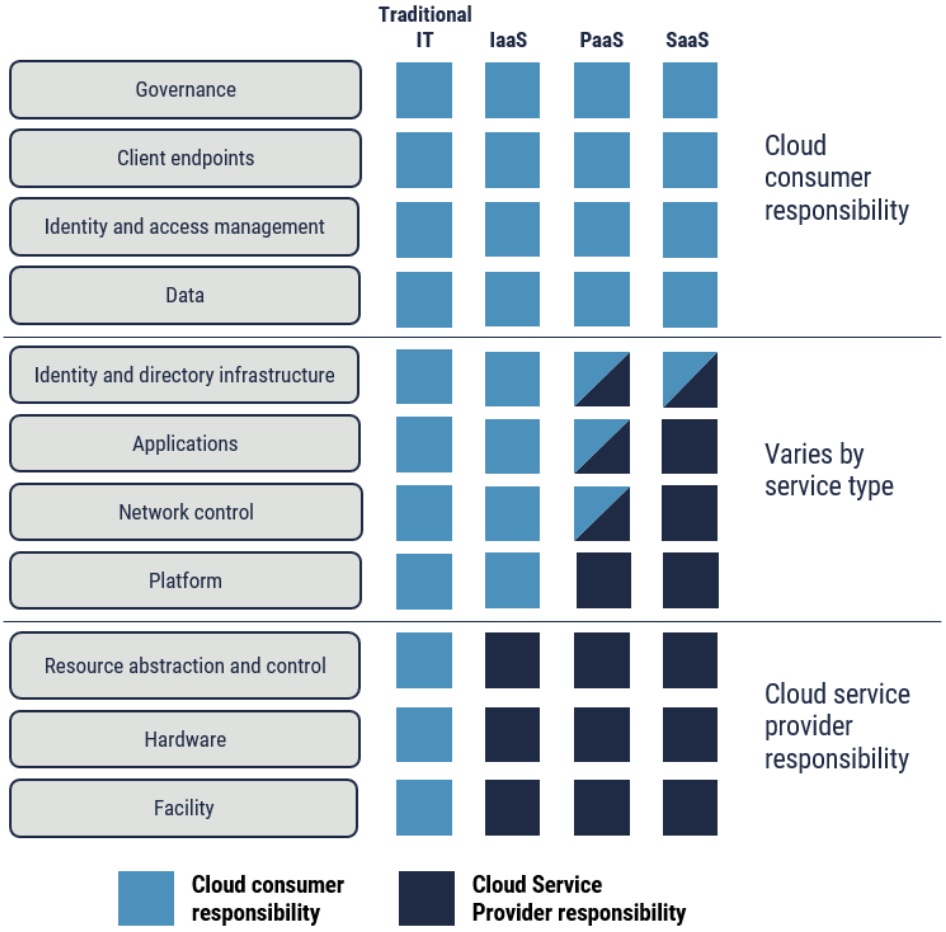


Figure Caption: Figure 1 represents the sharing of responsibilities between a cloud consumer organization and the CSP, breaking down the responsibilities in accordance with the cloud deployment model selected. Whether your organization and CSP agree to an Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) deployment model, you will have a mix of responsibilities solely for your organization, solely for the CSP, and responsibilities shared between your organization and the CSP.

[1] The official (ISC)2 Guide to the CCSP CBK, 2016, Domain 1 Architectural Concepts and Design Requirements Domain, p4.

3.2.1 Organization (consumer) owned or controlled tenancy

When it comes to tenancy ownership or control, the organization contracts directly with the main CSP, including for any PaaS or SaaS applications. In this context, your organization is therefore in direct control of the configuration of the tenancy and the requisite areas as noted in the shared responsibility model depending on what solution has been designed. One area of contrast is whether your organization contracts with an MSP or an MSSP that has access to your organization's administrative plane. While your organization owns and controls the tenancy, you provide the ability through your contract to the MSP or MSSP to then administer the tenancy on your organization's behalf. The extent of administrative control is dependent on your organization's intent. A key distinction between this arrangement or tenancy being hosted by another entity is that your organization maintains control and areas of liability will be negotiated.

3.2.2 Managed service provider and managed security service provider

The context of "being hosted" in a provider's tenancy or instance changes the dynamic of what your organization, as the consumer, may still be responsible for. Some of these areas of responsibility include identity and access control, and the data that is placed in the environment. The remainder becomes the responsibility or liability of the entity hosting the organization. The additional steps your organization can take beyond what has already been discussed is to establish whether your data is separated via logical or cryptographic measures. In the past, separate hardware configurations (server) were an option, but cloud environments do not offer this capability, unless a "bare metal" option is offered. This increases some complexities in the governance of your organization's operations, but it does alleviate the configuration and maintenance elements of the tenancy.

4 Conclusion

The use of cloud services can provide a great amount of flexibility and agility to your organization. There are many as-a-service offerings which have matured over the years, easing the transition to the cloud. As has been demonstrated in this guidance, there are areas of concern and questions that should be explored by your organization prior to, during, and after exiting a cloud environment. This guidance has been provided for general knowledge and guidance for any organization looking to begin their cloud journey and looking to sidestep pitfalls in the use of cloud technologies. As indicated, this is not to be taken as legal advice.

Overall, the key message is to work with your selected CSP to ensure common understanding of your engagement and to inquire and establish what can be done to meet your organization's specific needs.

5 Supporting content

5.1 List of abbreviations

Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
ASTRA	Analytical Software for Threat Assessment
CIS	Centre for Internet Security
CMVP	Cryptographic Module Validation Program
CSP	Cloud Service Provider
FIPS	Federal Information Processing Standard
HTRA	Harmonized Threat Risk Assessment
IaaS	Infrastructure as a Service
IAM	Identity Access Management
IDP	Identity Provider
IT	Information technology
LLM	Large Language Models
MFA	Multi-factor Authentication
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
PaaS	Platform as a Service
SI	Service Integrator
SO	Service Orchestrator
TLS	Transport Layer Security
TRA	Threat Risk Assessment

5.2 Glossary

Term	Definition
Artificial intelligence	A subfield of computer science that develops intelligent computer programs to behave in a way that would be considered intelligent if observed in a human (e.g. solve problems, learn from experience, understand language, interpret visual scenes).
Authentication	The process of verifying an identity claimed by or for a system entity.
Authorization	Access privileges granted to a user, program, or process.
Cloud computing	The use of remote servers hosted on the Internet. Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere.
Contract	A legally enforceable contract is a deliberate agreement (intention to create legal relations) constituted by, and unconditional acceptance of, an outstanding offer (offer of acceptance) involving a reasonably precise set of terms (certainty of terms) between two or more competent parties (capacity) that is supported by mutual consideration (consideration) to do some legal act voluntarily (legality of purpose).
Quantum computing	A quantum computer can process a vast number of calculations simultaneously. Whereas a classical computer works with ones and zeros, a quantum computer will have the advantage of using ones, zeros and "superpositions" of ones and zeros.
Threat and risk assessment	A process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats.

5.3 References

Number	Reference
1	Canadian Centre for Cyber Security. IT Security Risk Management: A Lifecycle Approach (ITSG-33). November 2012.
2	Canadian Centre for Cyber Security. Technology Supply Chain Guidelines (TSCG-01). October 2010.
3	Public Services and Procurement Canada (PSPC). Contract Security Manual.
4	United States Federal Risk and Authorization Management Program (FedRAMP). Control Specific Contract Clauses version 3.0. December 2017.
5	National Institute of Standards and Technology. Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-171) Revision 2. February 2020.
6	National Institute of Standards and Technology. Enhanced Security Requirements for Protecting Controlled Unclassified Information: Supplementary (NIST SP 800-172). February 2021
7	International Organization for Standardization. ISO/IEC 27001:2022 – Information security management systems.
8	International Organization for Standardization. ISO/IEC 27017:2015 – Guidelines for Information Security controls.
9	International Organization for Standardization. Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds as PII Processor.
10	Cloud Security Alliance (CSA)) Security Guidance for Critical Areas of Focus in Cloud Computing Version 4.0. July 2017

Number	Reference
11	Canadian Centre for Cyber Security. Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103). May 2020.
12	Canadian Centre for Cyber Security. Guidance on cloud service cryptography (ITSP.50.106). May 2020.
13	Canadian Centre for Cyber Security. Guidance on becoming cryptographically agile (ITSAP.40.018). May 2022.
14	Government of Canada. GC Cloud Guardrails – Protection of data-at-rest.
15	Government of Canada. GC Cloud Guardrails – Protection of data-in-transit.
16	Government of Canada. GC Cloud Guardrails – Data location.
17	Canadian Centre for Cyber Security. Guidance on cloud security assessment and authorization (ITSP.50.105). May 2020.
18	Canadian Centre for Cyber Security. Harmonized Threat Risk Assessments (HTRA).
19	Canadian Centre for Cyber Security. Cyber supply chain: An approach to assessing risk (ITSAP.10.070). July 2022.
20	Canadian Centre for Cyber Security. Supply chain threats and commercial espionage.
21	Canadian Centre for Cyber Security. Contracting clauses for telecommunications equipment and services (TSCG-01L).
22	International Organization for Standardization. ISO/IEC 27036 -– Cyber security –– Supplier relationships (Parts 1 to 4).
23	Canadian Centre for Cyber Security. User Authentication Guidance for Information Technology Systems (ITSP.30.031). April 2018.
24	Canadian Centre for Cyber Security. Top 10 IT Security Actions: Number 3 managing and controlling administrative privileges (ITSM.10.094). July 2022
25	National Institute of Standards and Technology. NIST SP 800-63-4 Digital Identity Guidelines: Federation and Assertions (Initial Public Draft). December 2022.
26	Canadian Centre for Cyber Security. Managing the risks to Government of Canada data when using cloud services (ITSM.50.109). August 2022.
27	Canadian Centre for Cyber Security. Guidance on defence in depth for cloud-based services (ITSP.50.104). May 2020.
28	Canadian Centre for Cyber Security. Guidance on cloud service cryptography (ITSP.50.106). May 2020.
29	Canadian Centre for Cyber Security. Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111). September 2022.
30	National Institute of Standards and Technology. NIST 800-123 Guide to General Server Security.
31	Center for Internet Security. CIS benchmarks.
32	Canadian Centre for Cyber Security. Securely configure devices. September 2019.
33	Canadian Centre for Cyber Security. Secure your accounts and devices with multi-factor authentication (ITSAP.30.030), June 2021.
34	Canadian Centre for Cyber Security. Cyber security at home and in the office: Secure your devices, computers, and networks (ITSAP.00.007. October 2020.
35	Canadian Centre for Cyber Security. Using your mobile device securely (ITSAP.00.001). December 2020.

Number	Reference
36	Canadian Centre for Cyber Security. How updates secure your device (ITSAP.10.096). March 2021.
37	Canadian Centre for Cyber Security. Cloud network security zones (ITSP.80.023). June 2023.
38	Canadian Centre for Cyber Security. Guidance on securely configuring network protocols (ITSP.40.062). October 2020.
39	Canadian Centre for Cyber Security. Network security logging and monitoring (ITSAP.80.085). December 2022.
40	Canadian Centre for Cyber Security. Cyber security considerations for consumers of managed services (ITSM.50.030). October 2020.
41	Canadian Centre for Cyber Security. Top 10 IT security action items: Number 2 patch operating systems and applications (ITSM.10.096). August 2022.
42	Canadian Centre for Cyber Security. Automatically patch operating systems and applications. September 2019.
43	Canadian Centre for Cyber Security. IT media sanitization (ITSP.40.006). July 2017.
44	Canadian Centre for Cyber Security. Addressing the quantum computing threat to cryptography (ITSE.00.017). May 2020.