Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

GUIDANCE ON DEFENCE IN DEPTH FOR CLOUD-BASED SERVICES

ITSP.50.104

May 2020

PRACTITIONER SERIES

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

FOREWORD

ITSP.50.104 Guidance on Defence in Depth for Cloud-Based Services is an UNCLASSIFIED publication, issued under the authority of the Head, Canadian Centre for Cyber Security. For more information, contact the Cyber Centre Contact Centre:

Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on (20/05/2020).

REVISION HISTORY

Revision	Amendments	Date
1	First release.	May 20, 2020

OVERVIEW

The shared computing paradigm offered by cloud computing enables organizations large and small to leverage a broad range of information technology (IT) solutions without the need for large upfront investment. Cloud computing provides a subscription-based model that allows for on-demand, self-service provisioning of IT resources.

These cloud computing characteristics have a significant impact on IT security risks, roles, and responsibilities. Security strategies must be carefully planned to avoid injury to an organization's business activities. Adopting cloud services requires organizations to understand the impact cloud adoption has on security controls, and adapt their security approach to address changes in each of these areas.

Cloud computing does not offer a simple solution to the protection of business assets. We recommend that your organization consider a layered approach when implementing security controls on its cloud workloads. Defence in depth provides a fundamental approach in protecting against the risks associated with the use of cloud computing. The objective of this security guidance document is to assist your organization in adjusting its security architecture and controls to the capabilities offered by the cloud, and to address the change in risk posture introduced by cloud adoption.

This document and its appendices will:

- review shared responsibilities and defence in depth terms and definitions;
- describe cloud adoption security benefits and areas of concern;
- describe architecture and security control considerations for the implementation and the operations of cloud workloads; and
- provide recommendations for each control area.

This document is part of a suite of documents developed by the Cyber Centre to help secure cloud-based services and supports the cloud security risk management approach defined in *ITSM.50.062 Cloud Security Risk Management* [1][1].

[1] Numbers in square brackets indicate a reference cited in the Supporting Content section of this document.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

Public and private sector organizations rely increasingly on cloud technology to achieve their business objectives. These cloud-based solutions are subject to serious threats that can have adverse effects on business activities. Compromises to cloud-based services can be expensive and threaten the availability, confidentiality, and integrity of information, information systems and business processes.

Security controls are critical elements in the design and consumption of cloud-based services. While many of the controls implemented in traditional infrastructure still apply to cloud environments, organizations must understand the differences cloud computing brings and adapt their security architecture and security controls accordingly. When used effectively, organizations can benefit from the rich set of security capabilities and features offered by modern cloud platforms. However, deploying security controls without considering the capabilities, the shared responsibilities, and the associated risks is likely to make cloud workloads less secure than traditional computing.

You can use the guidance in this document to help your organization adapt its security architecture and security controls to address the risks that come with cloud adoption.

1.1 POLICY DRIVERS

The primary policy driver for defence in depth is the effective protection of cloud-based services from cyber threats and vulnerabilities. The need for defence in depth is normally identified in security policies, directives, regulations, standards, and guidelines applicable to each organization. The publications identified below may be used as reference material when your organization is creating its own cloud security architecture and designing its security controls:

- Cyber Centre *ITSP.50.103 Guidance on Security Categorization of Cloud-Based Services* [2][2];
- National Institute of Standards and Technology (NIST) *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing* [3];
- NIST cloud computing reference architecture, which is documented in Special Publication 500-292 [4]; and
- Cloud Security Alliance (CSA) *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5].

1.2 APPLICABLE ENVIRONMENTS

The information provided in this security guidance document applies to private and public sector organizations. You can apply this guidance for all cloud-based services, independently of the specific cloud service model and cloud deployment models in use.

[2] Security control profiles have been developed for cloud-based services. These security control profiles are derived from the baseline profiles in Annex 4 of the Cyber Centre's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [6]. The cloud security control profiles are included in the annex in ITSP 50.103 [2].

1.3 RELATIONSHIP TO CLOUD RISK MANAGEMENT

Cyber Centre's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [6] suggests a set of activities at two levels within your organization: the organizational (departmental) level and the information system level.

As depicted in Figure 1, organizational-level activities integrate into your organization's security program to plan, assess, and improve the management of security-related IT risks faced by your organization. At this level, defence in depth supports organizational risk management by defining the security approaches of security control profiles. For more information on organizational-level activities, see Annex 1 of ITSG-33 [6].

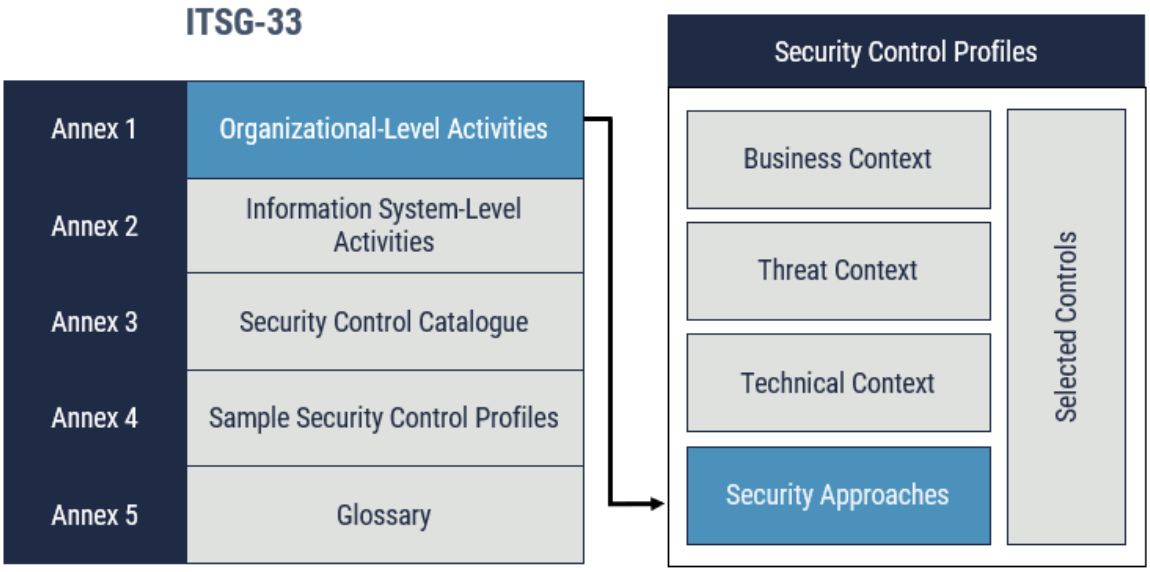

Figure 1: Relationship of Defence in Depth to Organizational Risk Management

Information system-level activities are integrated into an information system development lifecycle (SDLC). These activities include the execution of information system security engineering, threat and risk assessment, security assessment, and authorization. For more information on information system-level activities, see Annex 2 of ITSG-33 [6].

Cyber Centre's cloud security risk management approach is aligned with the information system level activities. As depicted in Figure 2, defence in depth supports step five of the cloud security risk management approach highlighted below. Defence in depth provides a layered approach that cloud service providers (CSPs) and your organization can use when designing and implementing cloud security controls.

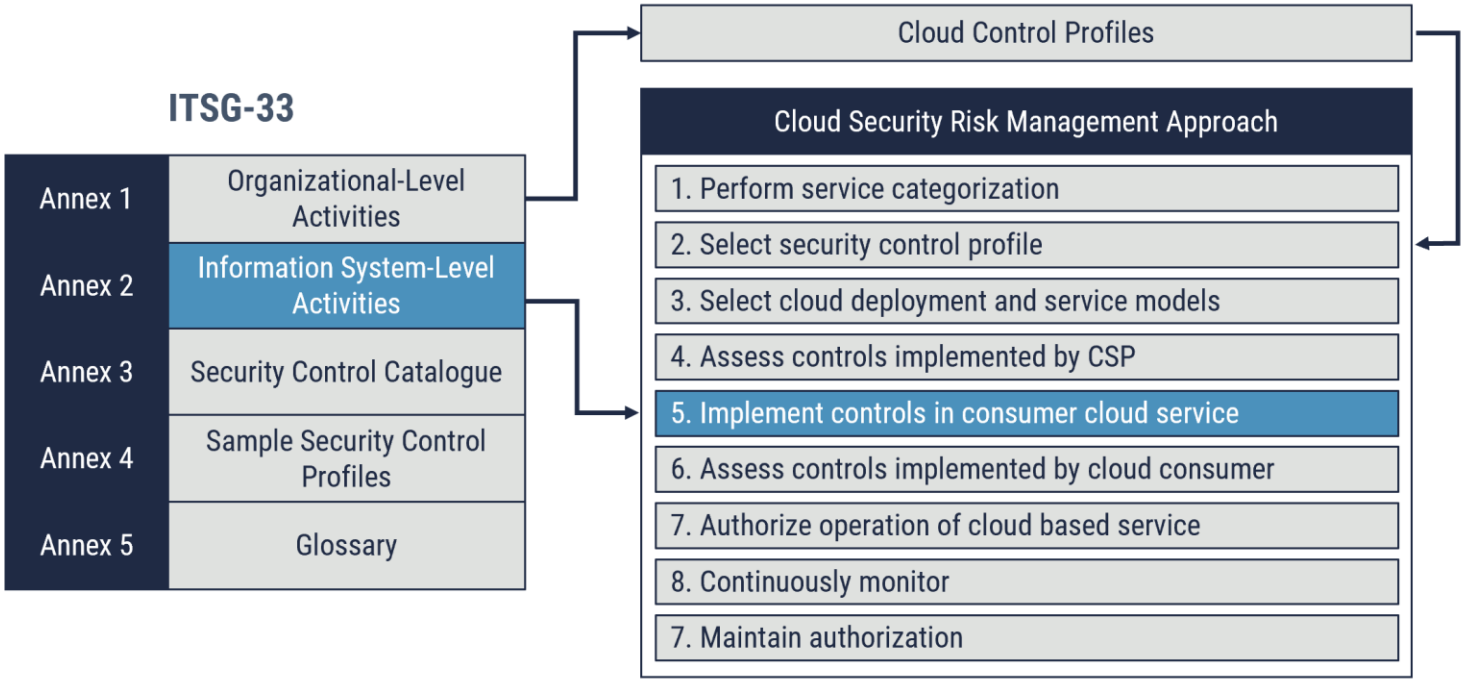

Figure 2: Relationship of Defence in Depth to Information System-Level Activities and Cloud Security Risk Management

2 CONTEXT

This guidance on defence in depth for cloud-based services is derived primarily from the following cloud computing and information system security risk management guidance:

- National Institute of Standards and Technology (NIST) *Guidelines on Security and Privacy in Public Cloud Computing,* documented in *Special Publication 800-144* [3]; and
- Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5].

2.1 WHAT IS CLOUD DEFENCE IN DEPTH?

The cloud security control profiles, which the Cyber Centre developed, define defence in depth as the strategic allocation of security safeguards (procedural, technical, or both) throughout the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective.[3]

To apply a defence in depth approach to cloud computing, your organization must understand the relationship of threats, vulnerabilities, shared responsibilities, and cloud platform capabilities to the recommended security controls. This helps protect the confidentiality, integrity and availability of business activities supported by cloud-based services.

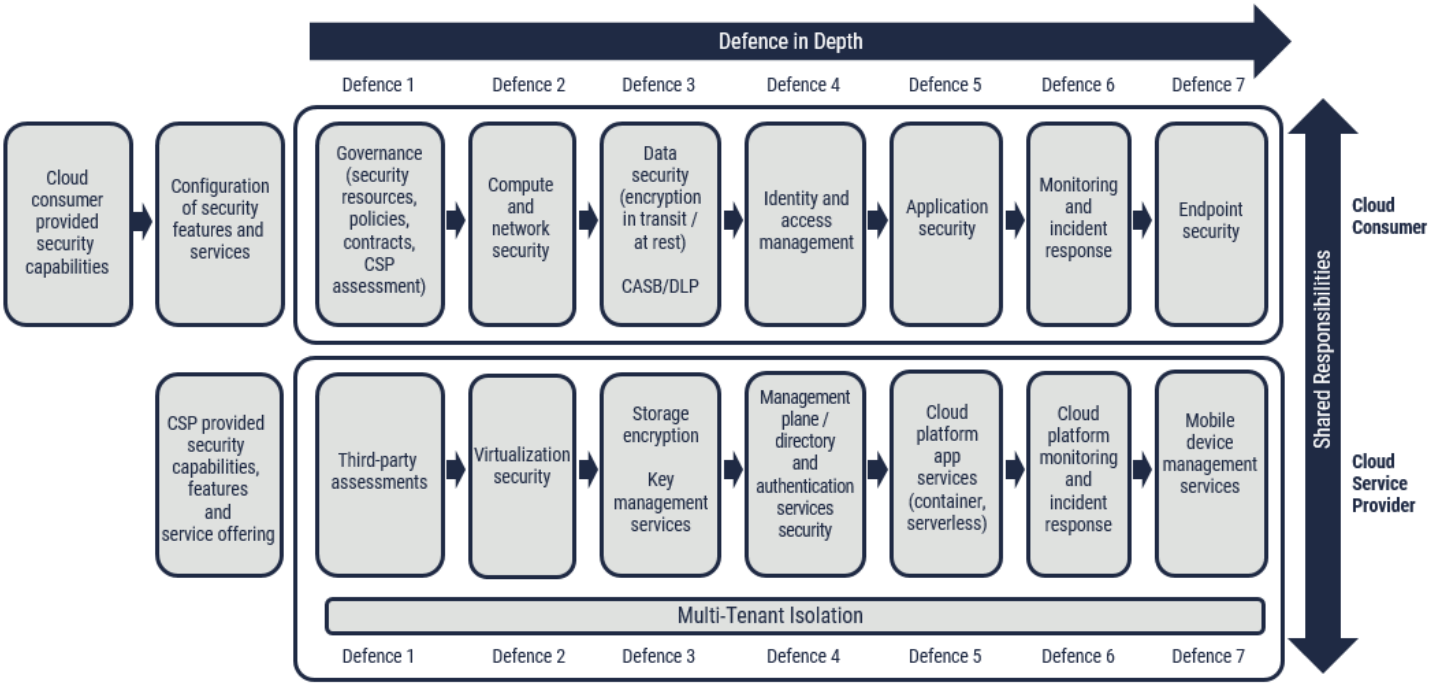

Figure 3: Cloud Defence-in-Depth Concept

[3] ITSP.50.103 [2] cloud control profile supplemental guidance for control PL-8(1) – Information security architecture - defence-in-depth.

2.2 CLOUD DEPLOYMENT MODELS

When deploying a cloud service, we recommend that your organization determine the appropriate cloud deployment and service model for its IT service. NIST *Special Publication 800-145* [7] provides detailed definitions of cloud computing that will be used throughout this publication. Cloud deployment models describe the relationship between the cloud service provider and cloud service consumer.

As depicted in Figure 4, there are four cloud deployment models identified by NIST: public, private, community, and hybrid. When selecting a cloud deployment model, we recommend that your organization consider several factors, including the flexibility, security, scalability, cost, and automation, level of control over the infrastructure, locality, and the service levels offered by each deployment model[4]. On premises refers to the software and technology located within the physical confines of your organization. Off premises refers to the software and technology located outside the physical confines of your organization. Cloud deployment model selection considerations are documented in ITSP.50.103 [2].

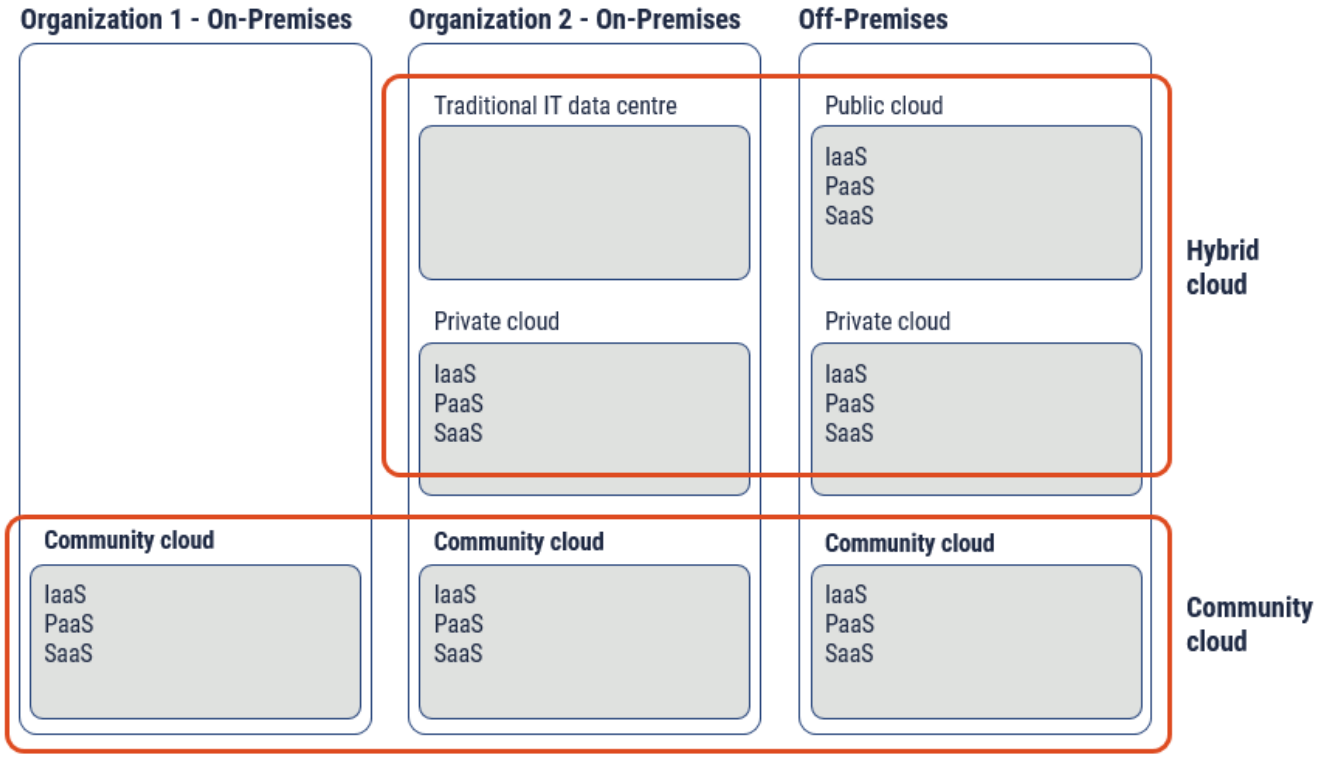

Figure 4: Cloud Deployment Models

[4] Cloud Standard Customer Council, *Practical Guide to Hybrid Computing* [8]

2.2.1 PUBLIC DEPLOYMENT MODELS

In the public deployment model, the cloud infrastructure is provisioned for the public's open use. The public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

2.2.2 PRIVATE DEPLOYMENT MODELS

In the private cloud deployment model, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). The private cloud may be owned, managed, and operated by your organization, a third party, or some combination of both, and it may exist on or off-premises.

2.2.3 HYBRID DEPLOYMENT MODELS

NIST describes the hybrid model as an environment composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. The combination of on-premises IT infrastructure with one or more of public, private, or community cloud is referred to as hybrid cloud.

2.2.4 COMMUNITY DEPLOYMENT MODELS

A community cloud is provisioned for exclusive use by a specific community of consumers from organizations with shared concerns (e.g. mission, security requirements, policy, and compliance considerations). The community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises. The costs are spread over fewer users than a public cloud (but more than a private cloud); therefore, only some of the cost savings potential of cloud computing is achieved.

2.3 CLOUD SERVICE MODELS

NIST defines three service models:

- **Software as a Service (SaaS)** provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface.
- **Platform as a Service (PaaS)** provides the consumer with the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the provider.
- **Infrastructure as a Service (IaaS)** provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources to where the consumer can deploy and run arbitrary software including operating systems and applications.

2.4 MANAGED VS CLOUD SERVICES

It is important to understand the key differences in control and shared responsibilities when comparing managed services and cloud services.

Managed services allow your organization to focus on its core competencies with minimal IT personnel and expertise while having the assurance that its IT infrastructure is managed properly. In traditionally managed services, organizations typically procure, own, and have full control of their equipment, software and other infrastructure components. The managed service provider (MSP) is responsible to perform tasks that your organization's IT personnel would normally do (e.g. outsourcing data backup and recovery, system monitoring and management, and patch management). The outsourced activities are normally performed at a lower cost, with a monthly fee based on the service being delivered.

With cloud services, your organization does not have to burden itself with investing in IT equipment and software. It uses the services on-demand, and pays per use for each cloud service it consumes. However, your organization still has the responsibility to securely configure, manage and operate the cloud services according to the cloud service model it has selected. As with traditional IT, if your organization does not have the personnel or expertise to purchase, deploy, secure, and manage its cloud services, it may opt to outsource these remaining responsibilities to a managed service provider.

2.5 SHARED RESPONSIBILITIES AND DEFENCE IN DEPTH

Understanding how the different cloud service models will affect defence in depth is essential. Your organization should not assume that it can shift most privacy, security, and compliance responsibilities to CSPs, and must understand its role in maintaining security of business services supported by the cloud. Figure 5 represents the sharing of responsibilities between a cloud consumer organization and the CSP.

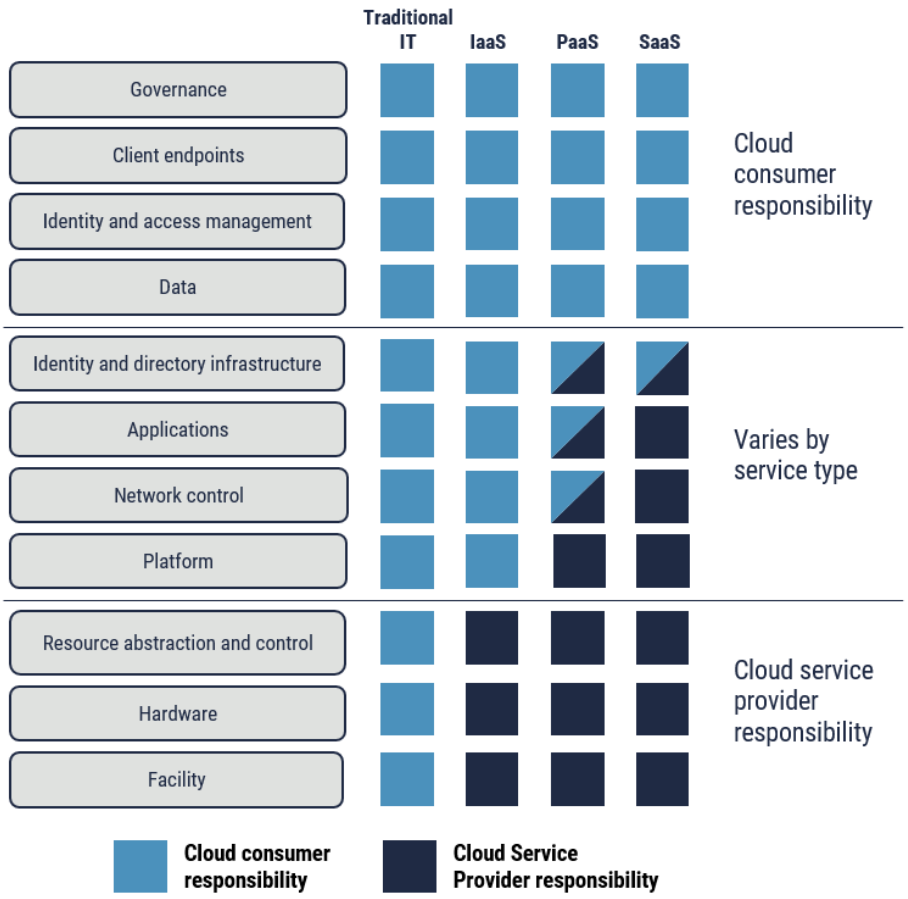

Figure 5: Shared Responsibilities and Defence in Depth

As described in Figure 5, when developing its defence in depth architecture, we recommend that your organization consider CSP managed and cloud consumer managed security controls.

Your CSP's managed security controls provide security **of the cloud** and protect the CSP's SaaS, PaaS, and IaaS product offerings. These controls help ensure:

- isolation and virtualization of the cloud infrastructure;
- security of the management plane;
- self-service portals and application program interfaces (APIs); and
- mechanisms which protect the cloud from physical and network threats.

CSPs are also responsible to provide your organization with key security capabilities including:

- data encryption at rest;
- identity and access management;
- secure key management; and
- multi-factor authentication.

Your organization is responsible for managed security controls that provide security **in the cloud**. Examples of security controls protecting cloud workloads include the following:

- web application gateways;
- network security groups;
- availability groups;
- storage encryption and tokenization;
- network security appliances;
- security baseline hardening; and
- configuration of CSP provided key security features and capabilities.

CSP and cloud consumer management responsibilities will vary based on the selected cloud service model.

3 CLOUD COMPUTING BENEFITS AND AREAS OF CONCERN

3.1 POTENTIAL BENEFITS

Although your organization has to surrender direct control for some portion of its IT infrastructure in its journey to the cloud, it can gain several potential security benefits through cloud adoption. Potential security benefits include[5]:

- **Security personnel specialization:** Small to medium sized organizations may not have the resources to develop expertise in every aspect of security and implement a multitude of security solutions. CSPs have clear incentives and resources to build experienced security teams and implement advanced security solutions to protect the cloud infrastructure and the services they provide.
- **Rich ecosystem of security capabilities:** CSPs generally develop and make available a rich set of security capabilities including encryption, high availability groups, and multi-factor authentication. Advanced capabilities can include advanced threat detection, security and compliance monitoring, and reporting.
- **Diminished reliance on manual tasks:** Modern cloud platforms offer many automation tools, templates, and scripting language that can be used to enforce and report on security baseline configuration. This means less effort to enforce compliance and fewer configuration errors.
- **Flexibility:** The deployment of security capabilities to multiple CSP data centres or regions is simplified and can be performed on-demand in multiple locations. Additionally, the implementation of temporary environments to test drive new security capabilities is greatly simplified.
- **Platform strength:** The consistency of cloud infrastructure facilitates deployment and automation of security controls which eases security baseline hardening, vulnerability management, security management, and incident response. In addition, an independent third party must formally certify a CSP. This third party confirms that the CSP meets various industry regulations[6].
- **Resource availability:** Public cloud provides very high scalability, which enables your organization to sustain periods of high demand and the ability to respond to distributed denial of service attacks. CSPs offer various high availability services to cloud consumers. This includes the capability to distribute cloud workloads to multiple data centres and virtualization hosts to protect workloads from infrastructure failures. CSPs also offer the capability to minimize the impact to cloud consumer workloads during periods of cloud infrastructure maintenance.
- **Backup and recovery:** Modern cloud environments generally provide storage, backup, and recovery capabilities that exceed those of your organization. Cloud platforms offer various data resiliency and replication features that your organization can configure to ensure geo-redundancy of data and backups. The backup and restore capabilities offered by CSPs may also allow your organization to achieve a faster recovery of data.

[5] Readers interested in a more detailed description of the security benefits are encouraged to consult NIST *special publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing* [3].
[6] Industry regulations such as Payment Card Industry Data Security Standard (PCI DSS), Service Organization Control (SOC) 1&2, Health Insurance Portability and Accountability Act (HIPAA), and the International Organization for Standardization (ISO 27001, 27017, and 27018).

3.2 POTENTIAL CONCERNS

While cloud computing may provide a number of security benefits, there are also some areas of added concern, including:

- **Complexity:** Cloud environments are much more complex than traditional computing environments. CSPs rely on a number of complex technologies to implement isolation and virtualization of cloud infrastructure, the management plane, and the necessary self-service interfaces for interactions with your organization. Additionally, CSPs provide key security features, tools, and the means for workload protection.
  - The potential lack of knowledge and experience with what may be new security features may increase the risk of misconfiguration of the cloud platform by your organization. We suggest that your organization invest in and develop the cloud security skills of its IT and security personnel. It should also understand which components are its responsibility and which are the responsibility of the CSP.
- **Lock-in:** By leveraging a CSP's key security features, your organization may find itself locked in to the CSP security service offering and may find it difficult to transition to a different CSP service offering.
- **Shared multi-tenancy:** Multi-tenancy generally requires sharing of compute, network, and storage resources. Any CSP infrastructure failures or configuration errors in the virtualization or isolation of these resources may impact the confidentiality, integrity, and availability of your organization's workload and data.
- **On-facing services:** The broad network access characteristic of cloud means that services are always exposed to threats from the Internet. In addition, on-premises Internet connectivity failures have the potential to impact your organization's access to the business services deployed on cloud infrastructure. We recommend that your organization consider implementing dedicated connectivity to reduce the risk of Internet connection performance degradation or failure.
- **Loss of control and visibility:** As a cloud consumer, you have limited control and visibility on the cloud components that are the CSP's responsibility. Such control and visibility may be important in areas where your organization shares its responsibilities with the CSP, and may be important in some compliance scenarios (e.g. security monitoring and incident response). We recommend that your organization understand the sharing of responsibilities between itself and the CSP. Concerns can be addressed through service level agreements (SLA), contracts, and CSP third party assessments.
- **Compliance:** We recommend that your organization fully understand its obligations under Canada's private sector privacy legislation, including those under certain pieces of provincial privacy legislation, and to carefully weigh the risks against the benefits.[7] Unless your organization is working with a Canadian-only CSP, you should also consider international regulations such as the European Union General Data Protection Regulation 2016/679 (GDPR) and the United States Cloud Act.

[7] Office of the Privacy Commissioner of Canada, *Cloud Computing for Small and Medium-sized Enterprises* [9].

4 CLOUD DEFENCE IN DEPTH CONSIDERATIONS

4.1 ISOLATION

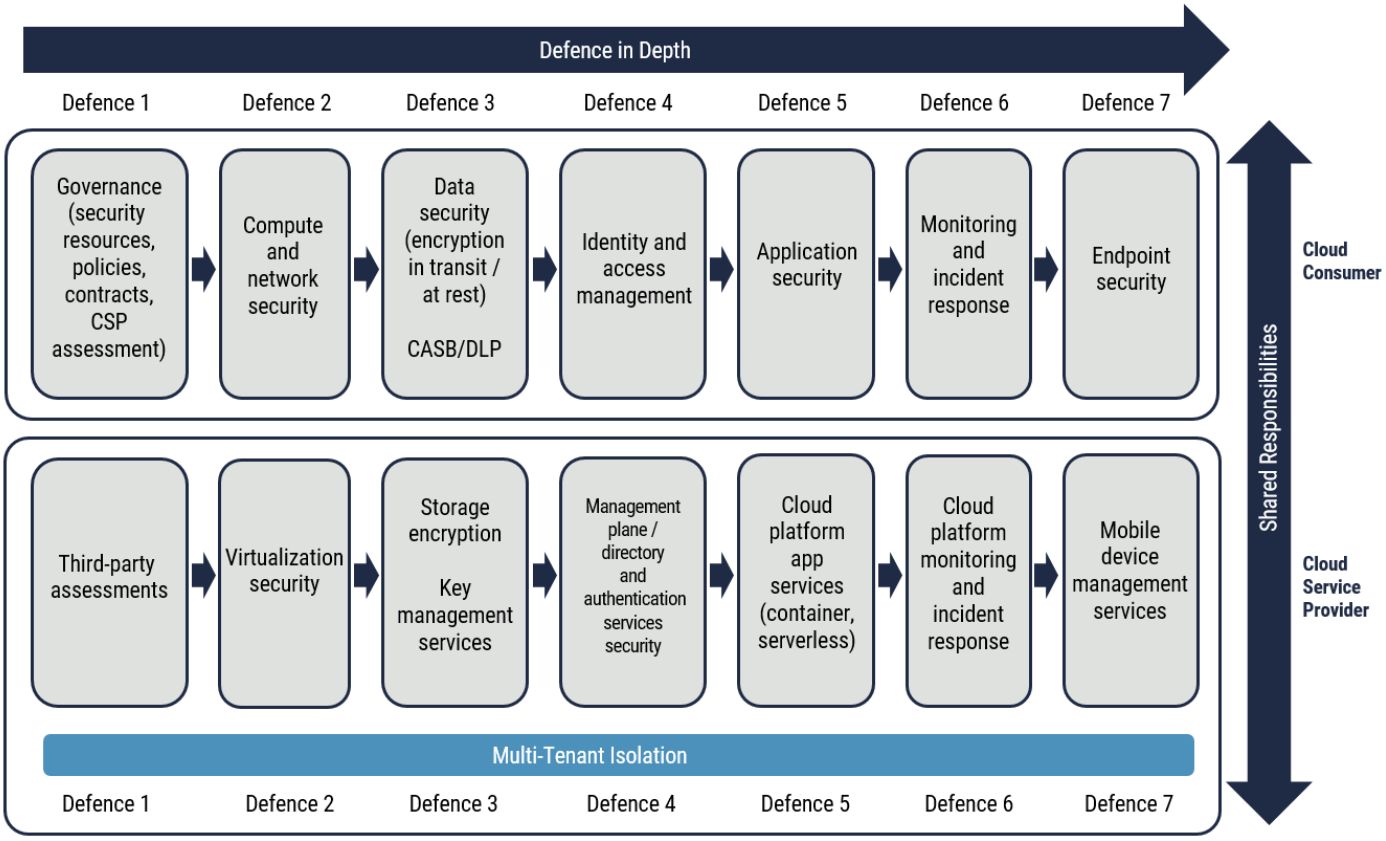

Figure 6: : Multi-Tenant Isolation

Cloud infrastructures are built on the premise that sharing a pool of resources between multiple customers will lead to economies of scale and translate into lower costs for your organization. This sharing of resources between multiple organizations is referred to as multi-tenancy (see Figure 6). In a multi-tenancy environment, it is crucial to ensure that tenants are isolated from each other to ensure that a security compromise to one tenant does not affect the confidentiality, availability, and integrity of other tenant workloads and data.

While CSPs are responsible to ensure isolation of resources assigned to each organization, it is important for your organization to understand how its CSP achieves isolation between tenants, and the level of isolation offered for each of their cloud services. This will allow your organization to select the appropriate cloud service design to attain the desired level of isolation and security. For example, CSPs frequently offer dedicated or shared instances of cloud services. Dedicated instances help increase the level of isolation. Your organization might be able to select a cloud service provisioned as a dedicated instance in its own virtual network using private addressing. This is in contrast to a service provisioned as part of a global pool of resources accessible via public addressing.

When leveraging many of the security features offered by your cloud provider, your organization should look for ways to increase the isolation between itself and your CSP, and between itself and other cloud consumer environments. For example,

we recommend that your organization consider deploying storage encryption, leveraging hardware security modules (HSMs) for protection of keys and secrets, and provisioning dedicated virtual machine (VM) instances.

4.2 CLOUD SECURITY GOVERNANCE AND RISK MANAGEMENT

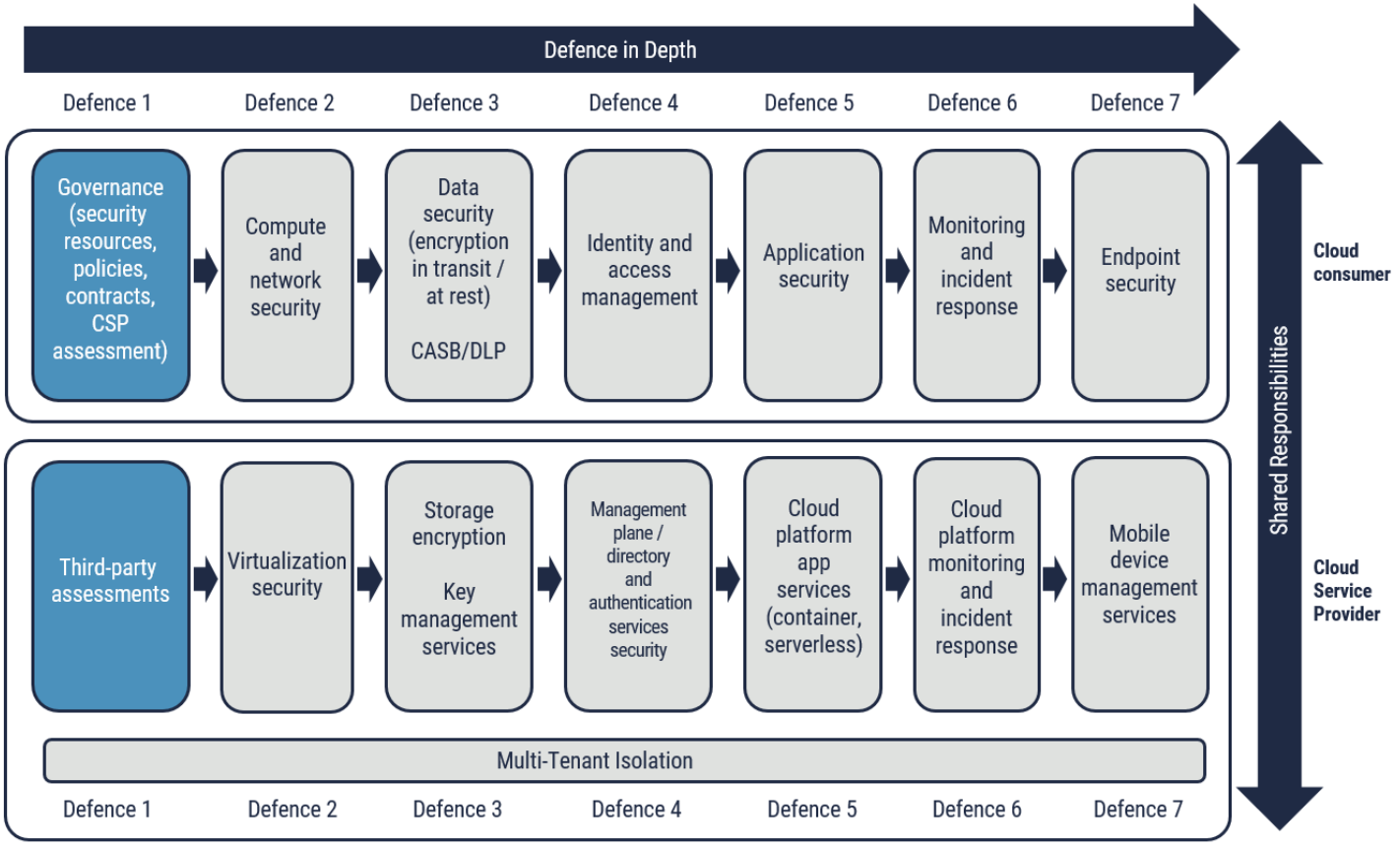

Figure 7: Cloud Security Governance and Risk Management

As seen in the previous sections, cloud computing brings a number of potential security benefits and concerns. With cloud computing, organizations do not have control or visibility over the CSP's technology, related policies, and procedures. Organizations may lack the necessary expertise to securely deploy cloud workloads. Without the necessary policies, processes, and standards to operate in the cloud, organizations may expose business assets to increased risks.

Cloud security governance and risk management provide the foundation to defence in depth. They govern the legal and compliance dimensions of the cloud transition, ensure clarity of roles and responsibilities, and provide the guiding principles for the protection of business processes and data against malicious actors. Your organization always retains governance responsibilities, which include the following:

- Allocation of security resources;
- Establishment of policies and guidelines;
- Formal third-party evaluations; and
- Cloud contracts.

4.2.1 ALLOCATION OF SECURITY RESOURCES

We recommend that your organization allocate sufficient security resources when adopting cloud computing. It should consider appointing cloud leaders to direct cloud core teams[8] that address the different aspects of the transformation (e.g. cloud security and risk management process, procurement, licensing, and roles and responsibilities). Senior management needs to communicate its support for cloud computing and encourage employees to develop their cloud security skills through both formal training and on the job exposure (with validation testing where possible).

4.2.2 ESTABLISHMENT OF POLICIES AND GUIDELINES

Your organization may assume that its current policies adequately cover the protection of business services and data deployed to cloud environments. However, when adopting cloud computing, your organization should not overlook the need for development of, or updates to, security policies and guidelines.

The realities of cloud adoption may require your organization to adapt its security policies to keep pace with the technological evolution. Aspects that may need to be re-examined include:

- acceptable use of cloud computing;
- acceptable cloud deployment and service models;
- roles and responsibilities;
- data residency;
- requirements for third-party assessments;
- contractual requirements;
- integration to identity management process;
- connectivity with external service providers;
- encryption and key management;
- data back-ups; and
- service decommissioning.

4.2.3 FORMAL THIRD PARTY ASSESSMENTS

As identified in ITSM.50.062 [1], your organization does not always have control or visibility of the design, installation, and assessment of the CSP's security controls. We suggest applying an alternative security assessment approach. This can be accomplished by considering other trusted security assessments. Results from these security assessments, if deemed applicable and reliable, can be incorporated into your organization's security assessments.

[8] Treasury board of Canada Secretariat, *Cloud Security Management Approach and procedure* [10]

In the context of the cloud security risk management approach, these trusted security assessments mainly consist of third-party attestations that have much more value than self-assessments. Common third party attestations cover various regulations and industry requirements[9].

These attestations require an independent third party that is bound to be objective and apply professional standards to the evidence it reviews and produces. However, third-party attestations rarely cover all security requirements identified in the selected security control profile. Additional security requirements and contract clauses may need to be included to ensure that the CSP provides the required evidence to support the security assessment activities.

These formal third-party attestations often require your organization to enter into a non-disclosure agreement and represent point-in-time assessment of the security controls and specific cloud provider services. It is important for your organization to monitor for any changes in coverage, status, and findings over time.

For more information on third-party assessments, please consult the Cyber Centre *ITSM.50.100 Cloud Service Provider Information Technology Security Assessment Process* [11].

4.2.4 CLOUD CONTRACTS

With cloud computing, your organization has a greater reliance on contracts to extend its governance to the cloud.[10]
We strongly suggest that your organization not underestimate the importance of the cloud contract. The cloud contract is your organization's primary tool to do the following:

- Extend its governance to the cloud;
- Document CSP and organization responsibilities;
- Document and enforce service level agreements (SLAs);
- Determine data ownership;
- Determine data residency;
- Determine third-party assessment requirements; and
- Address third-party assessment gaps.

The cloud contract should also include provisions that ensure your organization is notified of a security incident in a specific way and in a specific time.

To remain competitive, CSPs constantly develop and make new services available to organizations that may not be covered by existing contracts. Before using these new services, we recommend that your organization verifies that a third party has assessed these services. Your organization should also ensure that these services are covered in existing contracts. If not, then you should have the contracts amended before using new services.

[9] Industry regulations and requirements such as Payment Card Industry Data Security Standard (PCI DSS), Service Organization Control (SOC) 1&2, Health Insurance Portability and Accountability Act (HIPAA), and the International Organization for Standardization (ISO 27001, 27017, and 27018).
[10] Organizations will find more flexibility to negotiate cloud governance in a private cloud deployment model than with a public cloud deployment model.

4.3 NETWORK SECURITY

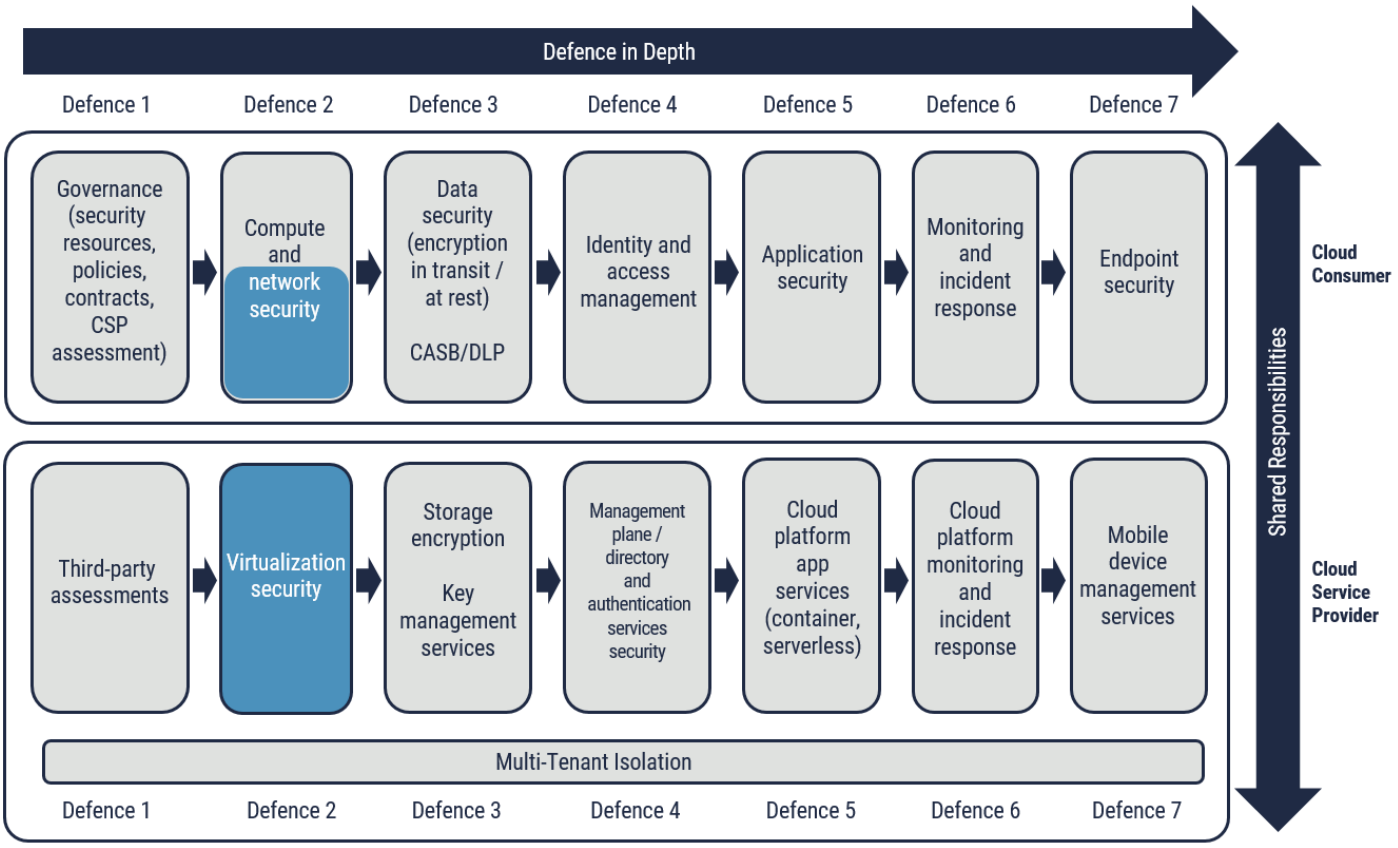

Figure 8: Network Security

4.3.1 NETWORKING SHARED RESPONSIBILITIES

Networking responsibilities include the management and security configuration of physical components, virtual networks, load balancers, network virtual appliances (NVA), domain name servers (DNS), and network gateways.

In all service models, CSPs are responsible for the implementation and management of network security controls to protect their cloud platforms from network threat vectors. Network safeguards implemented by CSPs normally include distributed denial of service (DDoS) protection, intrusion prevention systems (IPS), and firewalls. CSPs are responsible to implement the necessary network virtualization processes to ensure isolation between their cloud customers. CSPs must ensure any sensitive information is sanitized as virtual instances are released back to the shared pool of resources.

In the IaaS model, your organization is responsible to protect its virtual network from network threats. We encourage your organization to leverage and configure CSP security features or third-party offerings such as security groups, virtual load balancers, web application firewalls, and other third-party network security virtual appliances.

In the PaaS model, the CSP owns most of the management and security responsibilities. As a cloud consumer, your organization's responsibilities will vary based on the cloud services it chooses. For example, some CSP PaaS offerings allow

organizations to place the PaaS instance directly on the cloud consumer's virtual network. In these cases, we recommend that your organization leverage network virtual appliances or CSP network security features to protect access to its PaaS instance.

In the SaaS model, management and security of the network is a CSP responsibility and is included as part of the software offering. Your organization may be able to configure network restrictions using available SaaS security configuration settings, and limit access to its software instance to specific network locations (e.g. on-premises network only).

4.3.2 NETWORKING DIFFERENCES

The basic concept of cloud networking is based on software defined networks (SDNs). SDNs separate the network control function (i.e. the decision on where to send the packets) from the network forwarding function (i.e. the sending of the packets). The separation of the network control function allows it to be programmable, and offers much greater scalability and flexibility than traditional virtual local area networks (VLANs).

Cloud networking can impact security in a number of ways. For example, since the network control function is virtualized, network intrusion prevention systems (NIPS) cannot be implemented via physical port mirroring. NIPS functionality needs to be implemented via network virtual appliance (NVA) or host based sensors. Host based sensors are not available for all workloads. They can be easily defeated if the host is compromised, and offer limited management scalability. The use of NVA creates chokepoints as they must be deployed in-line to the traffic being monitored. This can potentially increase processor overhead on the NVA (requiring more powerful VMs to deploy the NVA functions) and increase costs. While some CSPs offer virtual tap services to monitor data flows, this does not generally provide the same capabilities as a physical network tap.

A number of cloud-native tools (e.g. network security groups) are usually made available by CSPs to facilitate access enforcement, network segmentation, and monitoring. However, many of these tools are not application layer aware. Third-party NVAs generally offer more mature and advanced capabilities than their cloud-native counterparts do, but they may not be designed with elasticity in mind. Trying to auto-scale these NVAs to match the elasticity and short lifespan of other cloud components can be challenging.

4.3.3 NETWORKING SEGMENTATION AND ZONING

Network segmentation plays a significant role in the protection of cloud workloads. Segmentation is a key approach supporting defence in depth and provides improved access control, monitoring, and containment. If an asset is compromised in one network zone, network segmentation limits the impact to assets in other zones.

The techniques employed differ from those used in traditional networking. It is common for cloud platforms to rely on software defined networking (SDN) for network segmentation, and to offer capabilities that were not possible in traditional networking.

CSPs usually provide a number of segmentation processes as part of their virtual network service offering. Your organization should understand the network segmentation methods available from its CSP, which could include capabilities to:

- configure subnets as public or private;
- provision each cloud workload and associated data in their own virtual network;

- provision dedicated instances of cloud services directly in cloud consumer virtual network;
- use cloud native security features to regulate traffic between segments (e.g. security groups);
- use NVA such as firewalls and load balancers to regulate traffic between segments; and
- regulate traffic based on tags or other attributes instead of IP addressing.

While developing its network segmentation strategies, we suggest that your organization use the features offered by its CSPs to limit lateral movement during a security breach. For example, your organization may want to create application workloads in their own virtual network, or further isolate workloads using security groups, thereby separating them from each other in a post breach scenario.

We strongly recommend that your organization **consider an assume-breach security model** and employ techniques such as micro-segmentation and software defined perimeter. With micro-segmentation, policies are implemented directly to VMs or applications via software. Policies are tied to VMs and applications instead of being implemented on a separate physical or virtual appliance such as a firewall. Even if the VM or application moves, the same policies are applied. Policies would no longer be tied to the network topology but rather be implemented at each component of the infrastructure. In essence, workloads are broken down into smaller units so that if one is compromised, the other ones are still protected.

4.3.4 ROUTING

In the IaaS model, routing is mostly a cloud consumer responsibility. Your organization is responsible for connectivity and network access control to compute, storage, data and cloud services. Routing is one of the primary mechanisms to control data flows and implement network security zones. Routing supports defence in depth by steering traffic to network virtual appliances, controlling data flows between virtual networks, and providing connectivity to on-premises networks.

SDNs provide CSPs unlimited possibilities when developing their virtual networking capabilities. Therefore, the network capabilities offered by service providers vary greatly from one provider to another. Your organization should understand how CSPs implement routing and how it can support network segmentation and security zones.

Improper understanding and configuring of routing behaviors can have serious security consequences. This is especially important in hybrid cloud deployments as the routing behavior may differ for each CSP. We encourage your organization to ask the following questions when designing and implementing its IaaS solutions:

- Are routes required to be explicitly specified before traffic is permitted between source and destination subnets?
- Is routing between all subnets allowed by default within a virtual network?
- Is there a default route to the Internet?
- Can virtual networks be provisioned without routes to Internet?
- How is connectivity to each subnet impacted when two virtual networks are peered together?
- Is a route required to force traffic to network virtual appliances?

4.3.5 HYBRID CLOUD NETWORKING

Client and business services hosted on off-premises cloud can be accessed via the public Internet; this can put business service availability and performance at risk. The reason for this is that your organization does not have direct control of security, reliability, bandwidth management, and latency of Internet connectivity.

As shown in Figure 9, CSPs offer private and dedicated network connections between on-premises infrastructure and connection exchange providers (CXP) locations. CXP locations act as the CSP's point of presence for private connectivity, and provide the following benefits:

- Dedicated bandwidth for cloud consumer use;
- Consistent and low latency connectivity; and
- Increased network security.

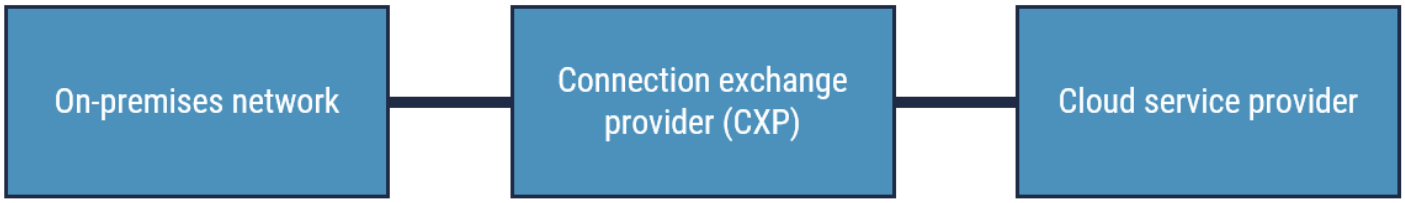

Figure 9: Private Connection to CSP via Connection Exchange Provider

When implementing private and dedicated network connections, we recommend that your organization ensure that adequate separation is in place to monitor and control traffic between on-premises networks and off-premises cloud environments. Separation is typically enforced via routing, access controls, firewalls, or NVAs between the two environments.

Bastion or transit virtual networks are frequently used in hybrid clouds to connect multiple virtual networks to on-premises data centers[11]. As depicted in Figure 10, the private and dedicated network connections between on-premises and the cloud terminate in the bastion network. The bastion network is then peered with the other cloud virtual networks. Bastion networks can be used to enforce separation via routing and may provide an appropriate location for your organization to implement access-control and additional security tools between the two networks. We encourage your organizations to also consider implementing similar controls on the on-premises side of the dedicated connection to protect on-premises services.

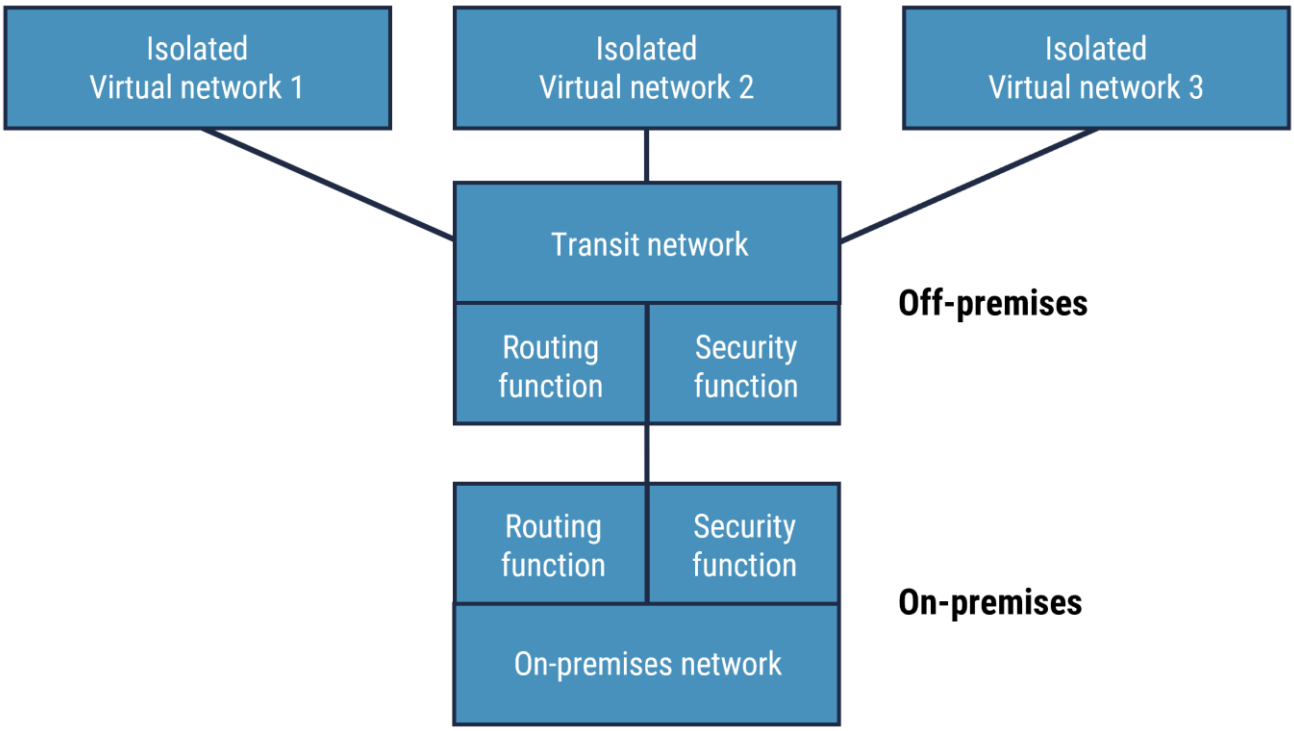

Figure 10: Bastion/Transit Network Concept

[11] Cloud Security Alliance Security *Guidance for Critical Areas of Focus in Cloud Computing* [5], section 7.3.5 Hybrid Cloud Considerations.

4.4 COMPUTE

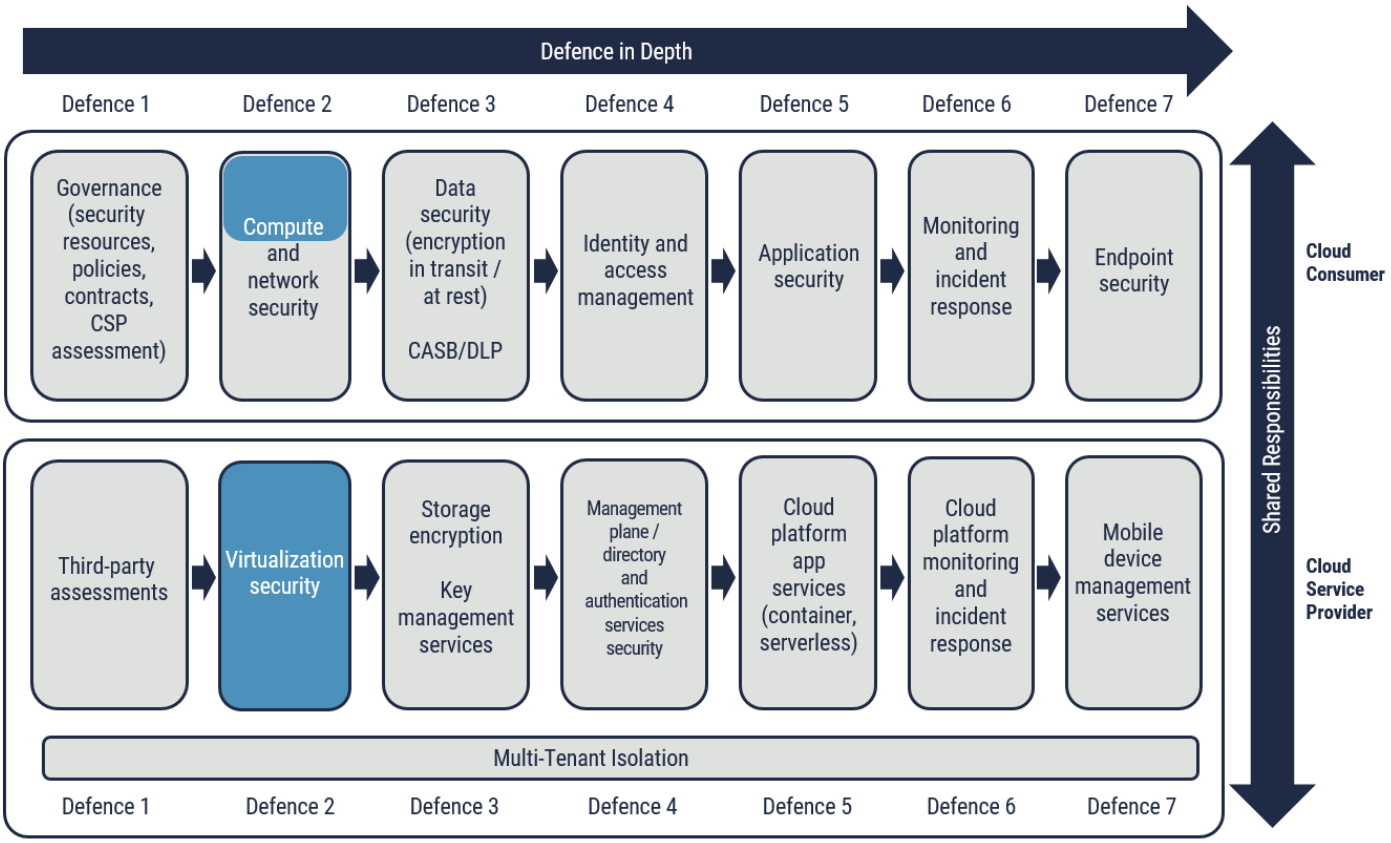

Figure 11: Compute

4.4.1 SHARED RESPONSIBILITIES

Compute responsibilities include the management and security configurations of the physical hosts, processors, hypervisors, virtual machines, containers, and server-less platforms.

CSPs are responsible for the security of the physical host, and the hypervisor. They must ensure that controls are in place to maintain workload isolation. In the SaaS and PaaS model, the CSP is mostly responsible for virtual machines and server-less workloads.

In the IaaS model, cloud consumers, like your organization are responsible for the management and security configuration of virtual machines. This includes patching, security baseline configuration, access control, identity management, and security monitoring.

The responsibility for container workload security will vary based on the service offering of each CSP. The responsibility falls with the CSP, the cloud consumer, or it can be shared between both.

4.4.2 DIFFERENCES

Compute workloads can be presented as a VM, a container, batch processing, high performance parallel computing, server-less computing, edge computing, or other platforms. We recommend that your organization be aware of security considerations for each type of workloads.

Most of the security controls deployed on-premises are still applicable to cloud-based VMs. However, there are a number of security considerations for cloud deployment. Your organization should:

- use multiple VMs and other high availability features in workload designs;
- take advantage of cloud automation capabilities to enforce VM security baselines;
- leverage auto-scaling for improved availability;
- use agents that support auto-scaling;
- avoid agents not built for the cloud (possible performance issues);
- notify CSPs before performing a vulnerability assessment;
- capture logs externally (workloads can be dynamic and short-lived); and
- deploy VMs in approved CSP regions.

For non-VM compute workloads (managed by service providers), your organization has little control and visibility to the CSP's basic infrastructure security. The CSP may offer a number of security options and controls to your organization but it may have:

- no ability to run software agents;
- limited visibility to logs; and
- no ability to perform vulnerability assessments.

4.4.3 IMAGE MANAGEMENT

Many virtual systems in today's cloud environment are disposable. They are continuously created, replaced, destroyed, and resized. Designs change frequently and solutions must be implemented in a short period of time. Elasticity and auto-scaling means that workloads are short-lived. Because of this, it does not make sense to apply security patches or changes to running workloads as they would be lost as soon as the workload is terminated. A new approach is needed for image management to address the unchangeable aspects of these workloads.

Organizations seeking to leverage auto-scaling and containers should look for new approaches to image management, including the following:

- frequent automated image updates to apply security patches and malware signatures;
- automated image security baseline enforcement during image creation;
- automated security testing during image creation; and
- disabled log-ins and restricted services before image deployment.

These new approaches to image management bring a number of improvements to security including the following:

- A less complex patching process;
- Configuration management automation;
- Repeatable and enforceable security;
- No security configuration drift;
- Validation of infrastructure before deployment; and
- Simple roll-back and recovery processes.

4.5 DATA SECURITY

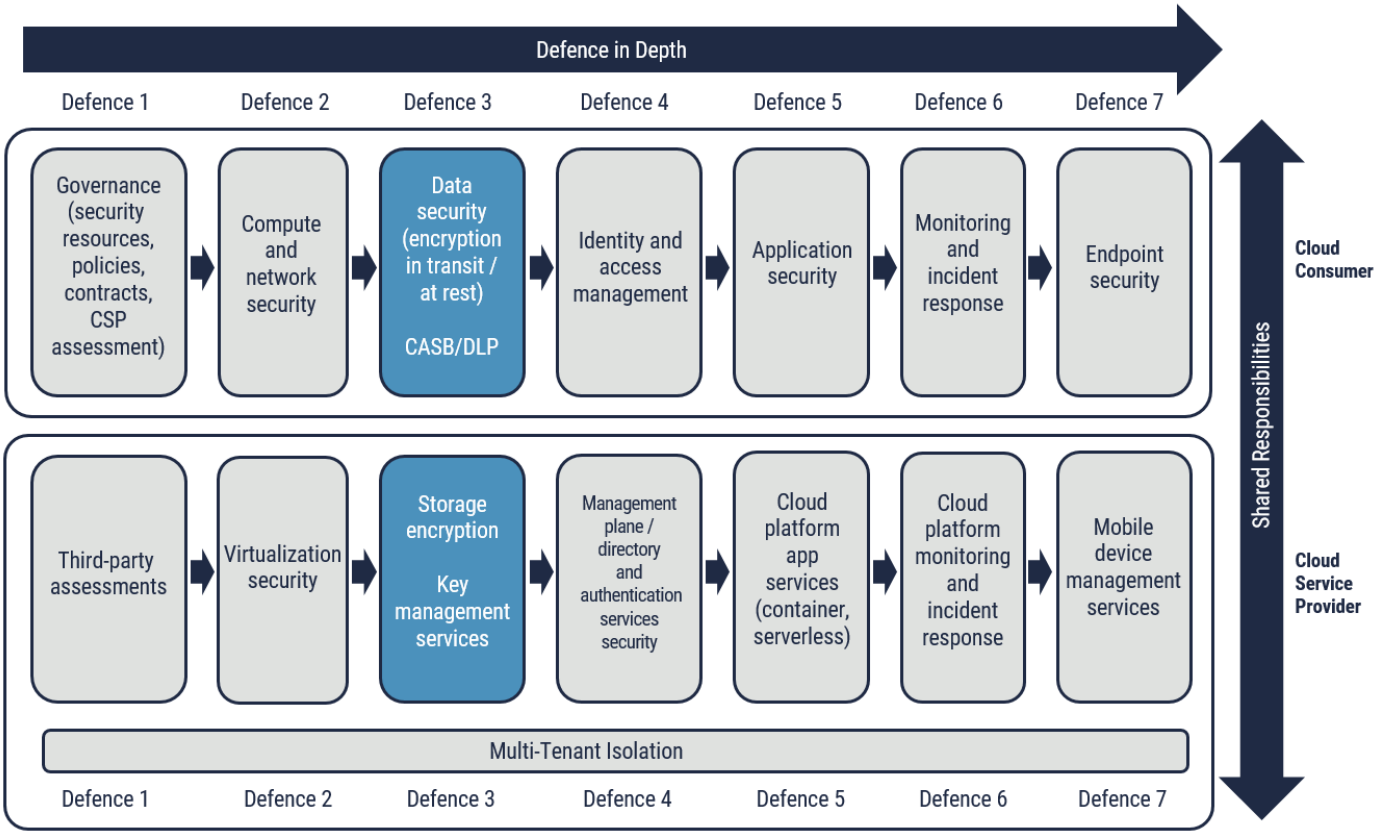

Figure 12: Data Security

Data security is one of the primary concerns for cloud consumers. Before hosting workloads and data on cloud platforms, cloud consumers should carefully plan and address data migration security strategy, data security while in the cloud, and security considerations for retiring or relocating applications on premises or to a different service provider. Data security is best addressed via a multilayer security strategy. Governance, infrastructure security, identity and access management, application security, and incident response management all play a role in data security.

4.5.1 SHARED RESPONSIBILITIES

Data security responsibilities include access control, encryption, key management, monitoring, lifecycle management, migration of data, and other cloud platform specific components.

Your organization is ultimately responsible for ensuring the security of sensitive data. Your organization is responsible for identifying the data allowed to be stored in the cloud, monitoring migrations, processing or storing of data on cloud infrastructure, and encrypting data as it is sent to the cloud. Your organization retains overall data lifecycle management responsibilities for data location, data residency, business continuity, and compliance and data privacy requirements. With the IaaS model, your organization is responsible for restoring data and backups.

CSPs are responsible for security of the storage infrastructure. They must ensure that controls are in place to maintain the isolation of storage accounts, the sanitization of media before disposal, and the sanitization of virtual storage before it's returned to the shared pool of resources.

CSPs provide a number of access control and key management service options to cloud consumers. In the PaaS and SaaS models, CSPs are generally responsible for restoring data and backups.

The responsibility for data at rest encryption will vary based on the service model and the type of storage.

4.5.2 DIFFERENCES

Many of the traditional approaches to securing IT infrastructure still apply to the cloud. One primary cloud security consideration is the type of storage available (e.g. block, file, and object storage). That said, virtualization also allows for additional storage options including:

- virtual hard drives for IaaS virtual machines;
- various database platforms for PaaS;
- various application storage platforms (e.g. table storage, message queues, caching); and
- content delivery networks (CDN).

Secure implementation of these storage solutions can be complex and can vary greatly between cloud storage services for each CSP. Your organization needs to understand that the default security configuration for these storage services is not always adequate. It needs to know the security configuration options for each of the storage services they plan to use. Common configuration options for storage security include:

1. **Data location**: For cloud consumers in the government sectors, regulated industries, or in countries with strict data protection laws, knowing the geographic location of the data stored in the cloud is something that should not be overlooked. While data location is generally known for private and community clouds, in the public cloud deployment model, it can be hidden from the cloud consumer unless the CSP has offered optional location restriction policies and the consumer has configured their account to request specific location restrictions.[12]
2. **Access protocol**: Cloud consumers access cloud data via Internet-based protocols. Since, cloud storage is not always configured to use a secure protocol by default, cloud consumers should ensure that secure protocols are configured (e.g. through HTTPS) to access cloud data.
3. **Public storage**: Cloud storage can generally be provisioned as public or private storage. Your organization should monitor for changes to storage permissions that mistakenly allow for public access.
4. **Storage access keys**: Private cloud storage services are generally accessed via storage access keys. Your organization obtains the storage keys via the management portal for each CSP. We suggest that your organization have a documented key management and key rotation process in place to prevent unauthorized disclosure of storage access keys and data.
5. **Service endpoints:** Many CSPs offer service endpoints to enable access to external storage services as an alternative to connecting to those services directly over the Internet. Your organization should use service endpoints to control access to external services whenever possible.
6. **Storage firewall**: Some CSPs offer the capability to restrict access to cloud storage via whitelisting or blacklisting of source IP addresses. Endpoints with allowed IP addresses will have access to the cloud storage after successfully authenticating. Your organization should leverage this capability to restrict cloud storage access to authorized networks when using private cloud storage.
7. **Data sanitization**: Cloud consumers do not have control of the physical storage media, and the sanitization of physical media by cloud consumers may not be possible as cloud resources are shared between multiple tenants. Cloud consumers should consider encryption of data at rest to ensure data is sanitized before returning cloud storage resources to the CSP shared pool of resources.
8. **Data at rest encryption**: Your organization should consider provider-managed encryption and storage options. However, for high-security environments, it should consider using customer managed keys. Please consult the Cyber Centre publication *ITSP.50.106 Guidance on Cloud Service Cryptography for more information* [13].

[12] NIST *Special Publication 800-146, Cloud Computing Synopsis and Recommendations* [12].

4.5.3 DATA MIGRATION

Data migration to the cloud can be a complex undertaking. Improper data migration activities can compromise the confidentiality, integrity, and availability of information. Improper data migration can also impact your organization's business processes and its journey to the cloud. Data migration risks include unauthorized disclosure of information, data loss, data corruption, extended downtime, and non-compliance issues. There are also many types and forms of data such as business data, metadata, application source code, and others that each have unique data migration requirements. Cloud consumers must take the necessary planning steps to address security risks before initiating data migration to the cloud. Migration starts with identifying the data that should be allowed on the cloud. We recommend that your organization support its migration planning activities by reviewing its security policies, compliance requirements, and categorization of business process and information assets[13]. Through this process, your organization should identify compliance, legal, contractual, and business constraints. It should also identify data residency and location requirements, retention obligations, and the security categorization of its information assets.

We encourage your organization to select a cloud security profile to match the security category of its information assets[14]. The cloud security control profile identifies the recommended security controls that the CSPs and cloud consumer should carry out to support cloud-based services.

The security of data is important while it's in the cloud, but also when it's being migrated to the cloud. For instance, prior to data migration, your organization should ensure that data is backed up, encrypted in transit, protected in temporary and final storage destinations, and data confidentiality and integrity is maintained throughout the migration.

In addition to planned migration activities, we recommend that your organization put in place mechanisms to monitor large data migrations and activities on an ongoing basis. Tools such as Database and File activity monitoring, Cloud Access and Security Brokers (CASB), URL filtering, and data loss prevention (DLP) can provide the necessary visibility to detect and prevent unauthorized data migration, and use of unauthorized cloud services.

4.5.4 DATA SECURITY IN THE CLOUD

4.5.4.1 MANAGEMENT PLANE SECURITY

The role of the management plane in data security includes the management of operations that can be performed on storage resources. Organizations should use role based access to control who can create, configure, and delete storage resources, including storage access keys.

4.5.4.2 DATA IN TRANSIT

Data flows to, from, and within cloud environments transit on network infrastructure outside of the control of your organization. Malicious threat actors can intercept these communications to compromise confidentiality and integrity of information. We strongly encourage your organization to ensure that data in transit is encrypted to maintain secure communications to and from cloud environments.

[13] ITSP.50.103 [2] recommends an approach to inventory and categorize business process and information assets.
[14] Your organization should select one of the cloud security control profiles developed by the Cyber Centre, and which are included in Annex A and Annex B of ITSP.50.103 [2].

While your organization controls the IaaS perimeter, the communication patterns are likely to include information exchange with cloud services outside of the perimeter. In addition, the location of instances involved in data transfers is unknown. For example, your organization's VM instances might be located in different CSP data centres, and communications may flow on network infrastructure beyond cloud consumer and CSP control. As such, data communications within a cloud environment should be encrypted if any sensitive information is to be exchanged.

While client side encryption can be used before a data transfer is performed, it is recommended to use HTTPS for end-to-end encryption to ensure integrity of data. We also recommend that your organization do the following:

- Use HTTPS protocol for access to cloud storage services and APIs;
- Disable weak encryption ciphers; and
- Enable other encrypted network protocols for application specific use cases (e.g. SMB for access to file storage).

4.5.4.3 DATA AT REST

Encryption at rest provides data protection when stored on physical or virtual media. It protects data from unauthorized disclosure or modification. Encryption of data at rest supports the overall defence in depth approach. While consumer organizations and CSPs may have implemented controls at various levels to protect data, encryption at rest provides an extra layer of defence should other security measures fail.

We highly recommended that encryption of data at rest be included in your organization's defence in depth strategy. Your organizational security policies should be updated to address the encryption of data at rest requirement and identify the class of data needing to be encrypted on cloud storage. We suggest that your organization consider the encryption of data at rest to protect confidentiality and integrity of data, VM images, applications, and backups.

In a multi-tenant cloud environment, encryption of data at rest can be used as a mechanism to further isolate data from other tenants and from the CSP. Your organization may have to implement encryption at rest in order to meet industry, privacy, and government regulations, and even some regulation compliance requirements. In addition, encryption at rest enables your organization to sanitize data before storage resources are returned to the CSP shared pool of resources.

The approaches used for data at rest encryption vary considerably between IaaS, PaaS, and SaaS. This is further complicated by the different techniques available for management of encryption keys. The CSA *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5] provides a good description of each data at rest encryption approach. Figure 13 summarizes the data at rest encryption options described by CSA. Please consult the Cyber Centre publication ITSP.50.106 [13].

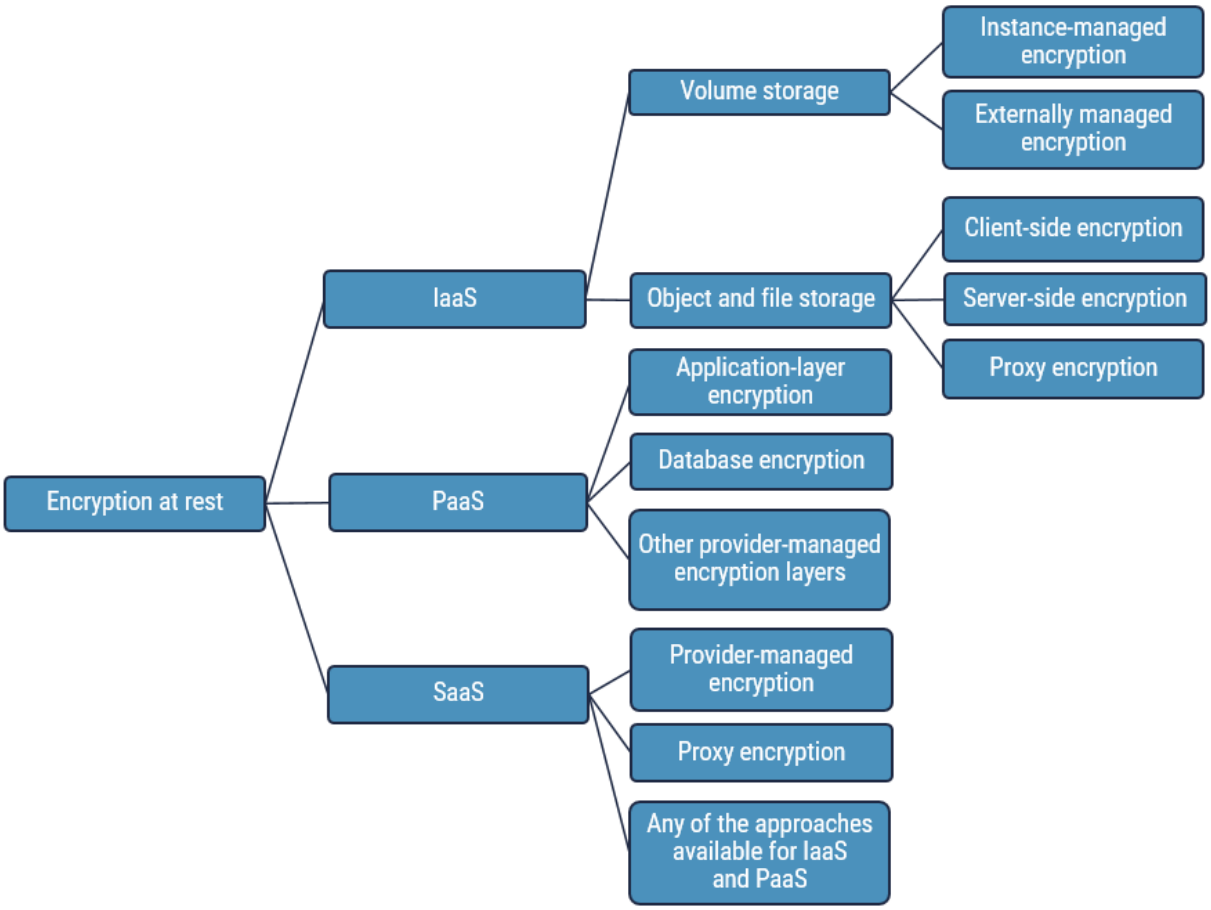

Figure 13: Data at Rest Encryption Approaches

Object and file storage encryption is often enabled by default by the CSP. However, default configurations can change over time. Your organization should enforce data at rest encryption through baseline security configuration and continuous monitoring. Any of the data encryption identified in Figure 13 will protect confidentiality and integrity of data against unauthorized access to physical media. However, not all of them will be effective against platform, operating system or application compromise.

Your organization should consider a number of factors when selecting its data at rest encryption strategy, including the type of data storage, the data environment (platforms, operating system, and application), the amount of data, and the threats to the data. For example, PaaS encryption options may vary from one platform to the other, while SaaS providers may use any of the options identified in Figure 13.

Key management is important for encryption of data at rest and should not be underestimated. Although complex, key management can be performed by the CSP or the cloud consumer. It involves the generation, distribution, storage, recovery, and destruction of encryption keys. An ineffective key management process can put confidentiality and integrity of data at risk, or worse, render the data unusable.

We recommend that your organization increase isolation from its CSP by managing encryption keys. Your organization should do the following:

- Ensure it has well designed, documented, and tested key management processes;
- Leverage its CSP key management service to simplify processes; and
- Consider a dedicated HSM option from its CSP for high-security environments.

4.5.4.4 DATA REPLICATION

Data replication provides durability and high availability[15] during planned and unplanned events, including disruptions related to power, hardware, network, and natural disasters.

Geo redundant storage ensures data is replicated to multiple geographic locations. Depending on cloud service provider offerings and options, data can be replicated within the same data center, to multiple data centers in the same region (not more than a few kilometers apart), or to multiple data centers in different geographic regions. CSPs normally offer some level of data replication by default, as well as a number of replication options. Your organization should understand the data replication options available and select the options required to meet their availability, durability and business continuity requirements.

4.5.4.5 DATA REMANENCE

Data remanence is the lingering representation of data that remains on a storage device even though efforts have been made to eliminate the data (e.g. overwriting, deleting, erasing). After data is eliminated, there are techniques that can be used to recover the data. Data remanence can make the unintentional release of sensitive information possible if the storage device is released, lost, or accessed without authorization. Your organization should protect the confidentiality of any residual data on storage media by ensuring it is disposed of properly. It may also be required by your organization to comply with its security policy, as well as privacy, government, and industry regulations.

NIST *Special Publication 800-88, Guidelines for Media Sanitization* [14], defines media sanitization as a process that renders access to target data on the media infeasible for a given level of effort. This ensures the continuing confidentiality of residual data on the media and minimizes the threat of unauthorized disclosure. In a multi-tenant cloud environment, your organization does not have control of the physical storage media. As such, media sanitization methods requiring physical access to media cannot be used by the cloud consumer. A different approach is required, for example, crypto erase (CE). The Cyber Centre publication *ITSP.40.006 v2 IT Media Sanitization* [15] identifies crypto erase as a sanitization process to erase the encryption key that is used on encrypted media, in order to make the data unreadable. CE is a method that can be used by the consumer to sanitize cloud storage media before it is released back to the CSP shared pool of resources.

[15] Western Digital defines storage availability as the storage *system uptime*, i.e. the storage system is operational and can deliver data upon request. Historically, this has been achieved through hardware redundancy. Durability, on the other hand, refers to *long-term data protection*, i.e. the stored data does not suffer from bit rot, degradation or other corruption. Rather than focusing on hardware redundancy, it is concerned with data redundancy so that data is never lost or compromised.

Encryption throughout the life cycle of the storage media facilitates fast and effective sanitization and eases the destruction requirements at the end of life of the media. We recommend that your organization routinely encrypt storage media throughout its life cycle to protect the ongoing confidentiality of data after media decommissioning and disposal. This ensures the continuing confidentiality of residual data on the media and minimizes the threat of unauthorized disclosure.[16] Your organization should consider HSM or the key management services offered by its CSPs to protect storage key encryption keys (KEK).

4.6 IDENTITY AND ACCESS MANAGEMENT

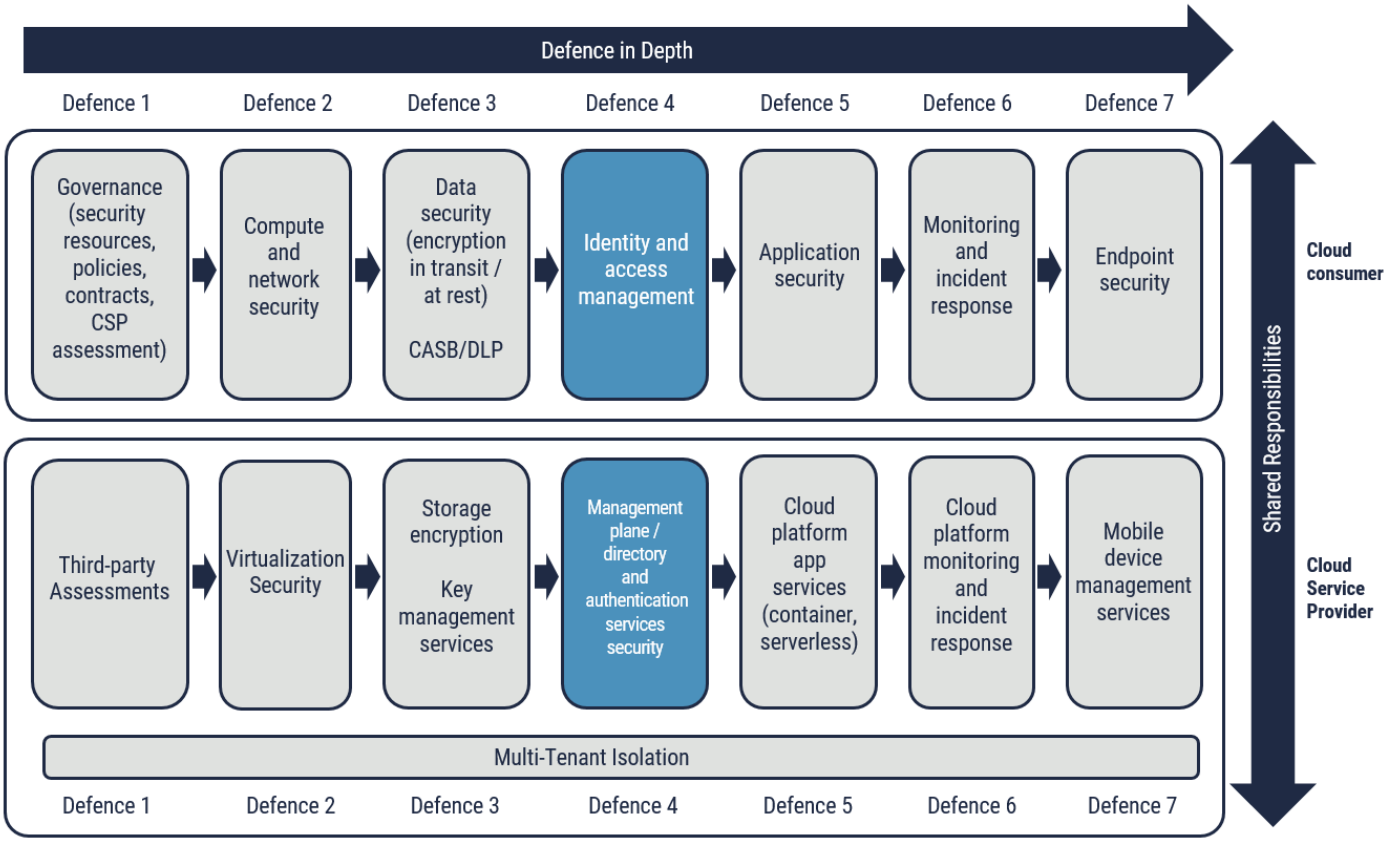

Figure 14: Identity and Access Management

Identity and access management (IAM) is among the most essential elements of protection in a defence in depth strategy. IAM can be thought of as who can do what with which resources and in which context. As shown in Figure 14, it is one of the key components that enable controlled access to resources, applications and information, and prevents accidental or malicious compromise of critical business assets.

[16] Cyber Centre *ITSP.40.006 v2 IT Media Sanitization [15]*

4.6.1 SHARED RESPONSIBILITIES

Identity and access management responsibilities include:

- establishing the identity provider (IdP);
- configuring the identity provider in cloud based applications;
- registering, provisioning, propagating, managing, and de-provisioning user identities;
- creating and managing access roles; and
- managing access to resources.

In the IaaS model, identity and access management is primarily the cloud consumer's responsibility.

In the PaaS and SaaS models, identity and access management is a shared responsibility. CSPs are generally responsible for implementation of directory and authentication services, application program interface (API) security, and the auditing function. Your organization is responsible for IAM policies, processes and procedures, and configuration of CSP provided IAM capabilities. It may also opt to leverage CSP or other third party IAM, single sign-on (SSO) and multi-factor authentication services.

In all service models, the CSP is responsible for enforcing the cloud platform management plane authorizations and access controls.

4.6.2 DIFFERENCES

4.6.2.1 FEDERATION

One key difference with IAM in cloud computing is that the CSP and the cloud consumer organizations share responsibilities. IAM in cloud computing requires identity management across various organizations and requires a level of trust between these organizations. Federation of identity addresses these challenges. Federation can be described as a Relying Party (RP) that delegates the authentication function to an IdP. For example, by delegating the authentication function to an IdP, a SaaS based application will use the assertion of a claimant's identity by the IdP to perform an authorization decision on whether to grant or deny access to the application. Through this process, your organization is able to provide an assertion confirmation of the claimant's identity to the SaaS application, without having to share user credentials or other user attributes with the CSP. The assertion of claimant's identity provided by the IdP can be trusted across multiple on-premises and cloud-based services to provide single sign-on capability.

4.6.2.2 GREATER NEED FOR STRONG AUTHENTICATION

Traditional on-premises IT environments rely on a well-defined trust boundary. To access applications and data, users have to be on the internal network and should be using a managed client device. With an increasingly mobile workforce where the use of personal devices is widespread, the traditional trust perimeter is ineffective. With cloud computing, the broad network access characteristic means that cloud based services can be accessed from any location and from any client device. In addition, the use of federation for single sign-on means that a compromise of user credentials may allow a threat actor to access and comprise a greater number of cloud based services from any location. In such an environment, relying on single factor authentication (e.g. username and password) leads to very high risks.

When adopting cloud computing, organizations should consider the use of multi-factor authentication to reduce the risk of account compromise[17]. This is especially important for privileged accounts and business-critical systems. For privileged accounts, we recommend that your organization consider credentials and authentication mechanisms providing a higher level of assurance[18], and restrict the management of cloud workloads through a separate access point, jump host, or both. A jump host is also known as a jump server. It offers controlled access between two dissimilar security zones.

4.6.2.3 STANDARDS AND PROTOCOLS

On-premises environments generally rely on directory access protocols (e.g. lightweight directory access (LDAP) and Active Directory) and authentication and authorization protocols (e.g. Kerberos). Cloud environments often need to be accessed from anywhere over the Internet. Authentication must be possible across firewalls without changes to firewall configuration. The authentication protocol should also be able to recover from Internet network failures. Commonly supported standards and protocols include Security Assertion Markup Language (SAML), and Open Authentication Standards (e.g. OAuth, and OpenID).

4.6.2.4 ACCESS MANAGEMENT

Traditional on-premises access management is generally implemented via role-based access control (RBAC). RBAC most often relies on a single attribute (role) to grant access. This approach does not provide the flexibility and security required for users who need access from anywhere using a multitude of devices. Additional contextual factors need to be considered in access management policies and decisions such as the availability and expertise of your organization's information technology security (ITS) personnel and the security requirements of your services and data.

Attribute based access control (ABAC) allows more granular and context aware decisions. In other words, access control decisions are made by incorporating multiple attributes, such as role, location, authentication method, device compliance, and more[19].

CSPs commonly provide more ABAC support as part of their IAM offering. As a cloud consumer, your organization should prefer ABAC to RBAC solutions for the greater flexibility and finer granularity they provide in implementing access policies and decisions in rapidly changing cloud ecosystems.

[17] For more details on multi factor authentication, organizations may want to consult the Cyber Centre *ITSP.30.031 V2 – User authentication guidance for information technology systems* [16], and NIST *special publication 800-63-3, Digital Identity Guidelines* [17].
[18] For more information on credential and authentication level of assurance, readers are encouraged to consult the Cyber Centre *ITSP.30.031 V2 – User Authentication Guidance for Information Technology Systems* [16].
[19] A more substantial explanation of ABAC can be found in NIST *Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations* [18]

4.7 APPLICATION

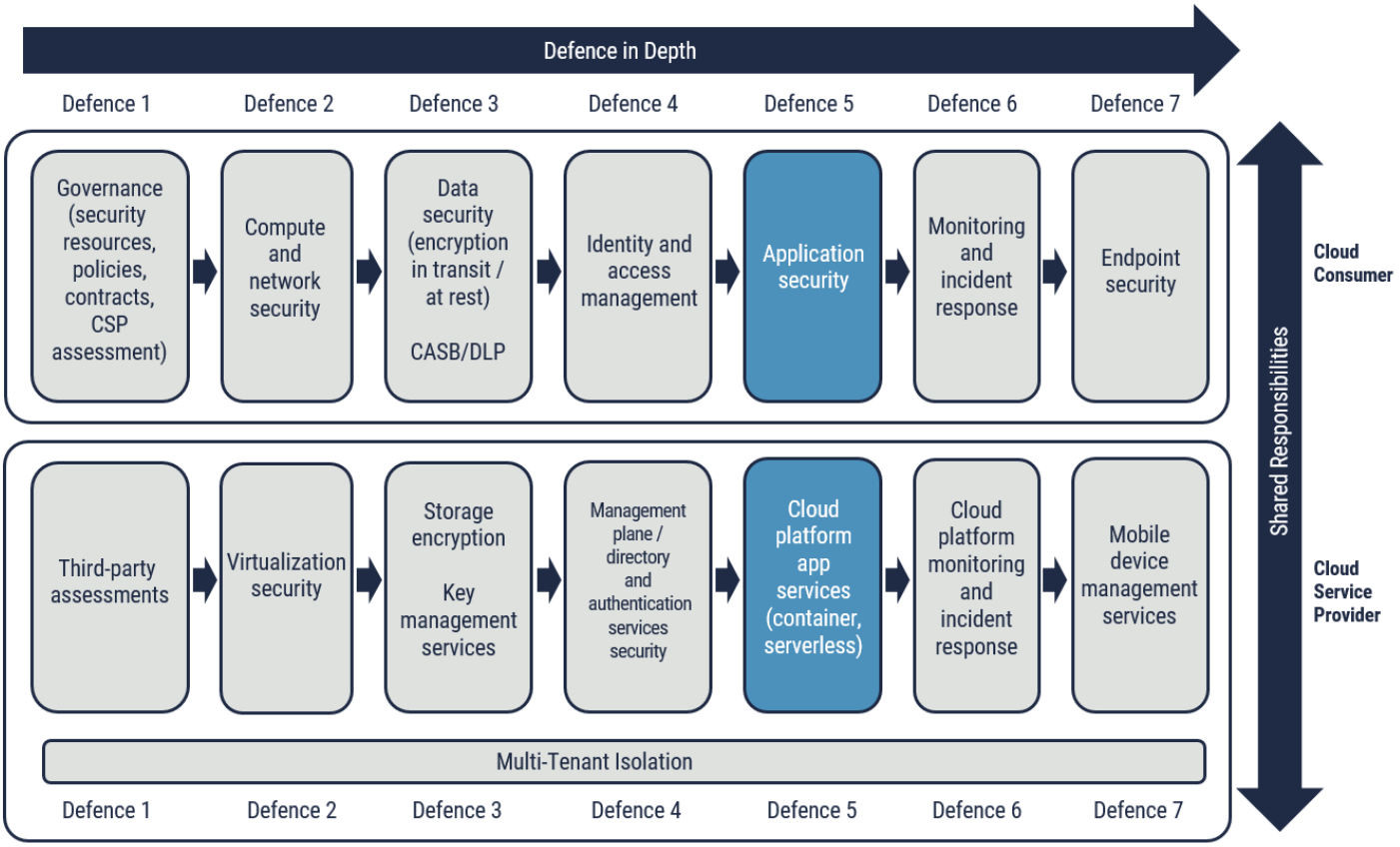

Figure 15: Application

4.7.1 SHARED RESPONSIBILITIES

Application security responsibilities include secure application development, source code analysis, security and vulnerability testing, secure deployment, runtime vulnerability management, and threat protection.

In the SaaS model, CSPs are responsible for all aspects of application security, while your organization remains responsible for configuring those services correctly.

In the IaaS and PaaS models, your organization (the cloud consumer) is responsible for application security. CSPs provide the functions and services to help secure access and your organization needs to configure and establish the secure access rules, including group and individual rights.

4.7.2 DIFFERENCES

When used properly, cloud computing capabilities have the potential to improve application security overall. To meet this objective, we recommend that your organization implement a number of changes to application development policies, software development life cycle, design patterns, and security operations.

Organizations should develop a cloud application security architecture and pre-approve cloud application security design patterns with specific attention to: API Security, management plane security, encryption, IAM, and new cloud computing security models. Organizations may need to customize or update legacy applications before migrating them to cloud services to effectively leverage and secure them.

Organizations should ensure application development, operation, and security personnel are trained on cloud security fundamentals and cloud provider technical security services and capabilities.

The CSA *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5] provides detailed coverage of application security differences and considerations in cloud computing. Notable security considerations include[20]:

- moving to a continuous deployment process and automating security (including security testing into the deployment pipeline);
- automating security in deployment and operations;
- scrutinizing API calls to the cloud service and management plane;
- ensuring that only least privilege entitlements are enabled;
- accounting for CSP cloud platform features, services, and security capabilities in security plans;
- ensuring no static embedded credentials in application code;
- leveraging KMS and HSM for secret and key management;
- leveraging micro-services security and architecture to facilitate workload lockdown and minimize the services running on them; and
- leveraging server-less computing security and architecture to reduce the attack surface.

[20] For a detailed coverage of application security differences and considerations in cloud computing, readers should review Domain 10 of the CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5]. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

4.8 MONITORING AND INCIDENT RESPONSE

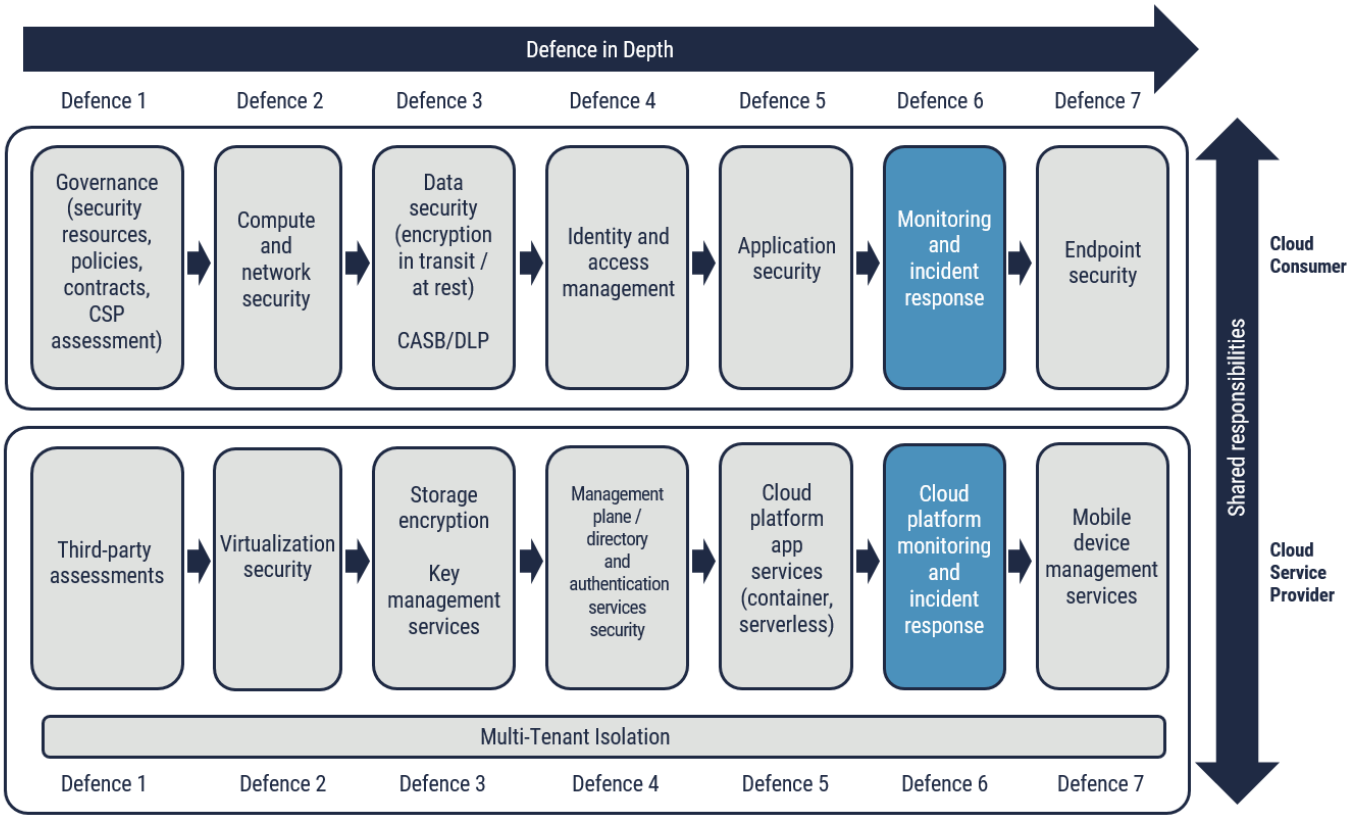

Figure 16: Monitoring and Incident Response

As shown in Figure 16, despite all of the controls implemented to protect the cloud environment, a good defence in depth strategy would be incomplete without security monitoring and incident response. Organizations must ensure that they put in place the policies, personnel, procedures, and technology to recognize, respond to, mitigate, and recover from security incidents.

4.8.1 SHARED RESPONSIBILITIES

Both the CSP and the cloud consumer are responsible for monitoring and incident response. Their level of responsibility will vary according to the service model (IaaS, PaaS, or SaaS).

CSPs are responsible for monitoring the cloud platform. CSPs are to notify cloud consumer organizations when the infrastructure hosting their cloud services is affected by a security incident, and to establish a point of contact for incident response communication. CSPs can also offer security monitoring options, which your organization can use to support its own monitoring and incident response activities.

In an IaaS model, your organization is responsible for monitoring network interfaces and security virtual appliances, security events from VMs, applications, authentication systems, databases, and provisioned cloud services, including management

plane and API security events. Your organization is responsible for incident response activities and notification to affected users.

In the PaaS model, your organization's responsibilities include monitoring of applications deployed on PaaS, including management plane and API security events. Your organization is also responsible for incident response activities and notification to affected users.

In the SaaS model, your organization's responsibilities are generally limited to monitoring of the SaaS instance, notifying affected users, and working with the CSP to restore operations.

4.8.2 DIFFERENCES

The adoption of cloud computing impacts each phase of the monitoring and incident response life cycle. Factors driving changes to the incident response approach include:

- loss of control due to shared responsibility model;
- service level agreement, response time and coordination with CSP;
- potential for absence of direct point of contact with service provider (may have to rely on standard support contact);
- short lived instances (impacting forensics and logging activities);
- potential gaps in availability of logs and data for components under CSP responsibilities;
- potential benefits of cloud automation and isolation capabilities to incident response; and
- availability of service provider tools to support incident response.

The Table 1 provides a summary of monitoring and incident response considerations in cloud computing[21].

[21] The information in this table is based on information from domain 9 of the CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5].

Table 1: Monitoring and Incident Response Considerations in Cloud Computing

Incident lifecycle phase	Cloud security consideration
Preparation	• Understand SLA and coordination with CSP. • Test the incident response process with the CSP. • Validate that escalations and role responsibilities are clear. • Ensure the CSP has contacts to notify your organization of incidents they detect, and that such notifications are integrated into your organization's processes. • Ensure to maintain and test contacts (including out-of-band methods) for communication with CSP. • Understand and document what data and logs will be available in an incident for each service. • Architect the cloud environment for faster detection, investigation, and response.
Detection and assessment	• Ensure monitoring scope covers the cloud's management plane activities. • Leverage in-cloud monitoring and alerts to speed up the response process. • Integrate cloud platform logs into organization security operations/monitoring. • Understand what is logged and the gaps that could affect incident analysis. • Login frequently to cloud workloads to address gaps in the visibility to cloud platform logs. • Understand potential chain of custody issues in forensics and investigative support. • Automate forensic or investigation processes in cloud environments to address dynamic and higher-velocity of cloud workloads (e.g. VM snapshots). • Leverage the capabilities of the cloud platform to determine the extent of the potential compromise (e.g. network flow, configuration data, and access logs).
Containment, mitigation and recovery	• Ensure the cloud management plane is free of an attacker. • Leverage cloud platform capabilities to speed up the quarantine, eradication, and recovery process. • Confirm that the templates and configurations for new infrastructure applications have not been compromised.
Post event activity	• Work with your organization's internal response team and CSP to figure what worked and what did not. • If agreed-upon response time, data, or other support wasn't sufficient, consider renegotiating SLAs.

4.9 ENDPOINT SECURITY

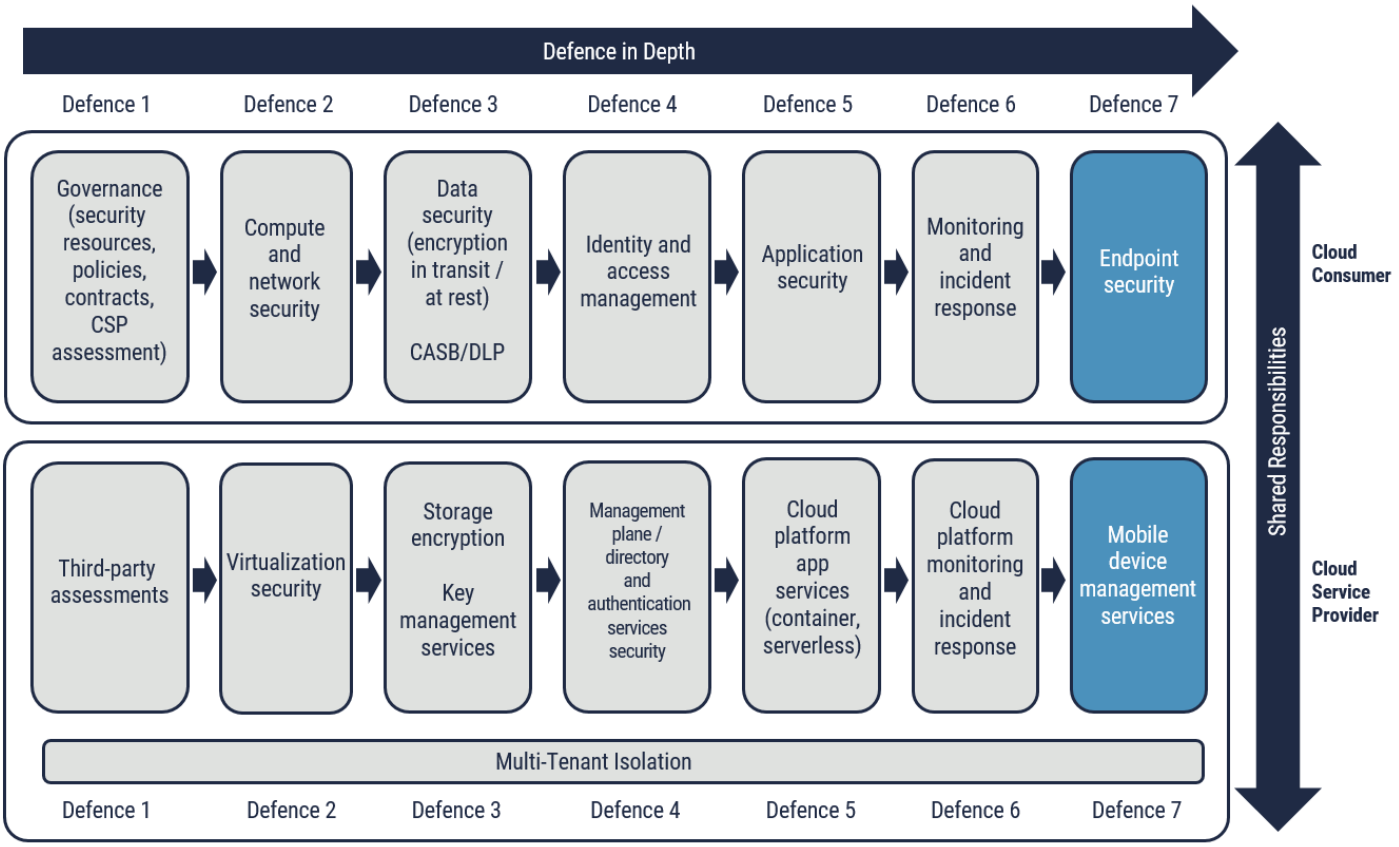

Figure 17: Endpoint Security

Your organization is always responsible for the security of the endpoint devices (with which users access cloud services). However, CSPs may provide the capabilities to manage endpoint devices through a cloud-based mobile device management (MDM) solution. In such cases, your organization has the responsibility for defining security requirements for the devices, and the CSP is responsible for enforcing those requirements via the MDM solution.

5 SUMMARY

Cloud defence in depth requires your organization to architect its cloud deployment strategy. Development of an efficient architecture requires your organization to have an understanding of shared responsibilities, cloud deployment models, cloud service models, threats and vulnerabilities, cloud platform architecture, and security capabilities. This document can help your organization understand the architectural considerations necessary for ensuring a secure deployment of business services on cloud platforms.

5.1 CONTACTS AND ASSISTANCE

If your department needs guidance on a defence in depth approach for cloud services and would like more information, please contact:

Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
API	Application Programming Interface
CSA	Cloud Security Alliance
Cyber Centre	Canadian Centre for Cyber Security
CE	Crypto Erase
CSE	Communications Security Establishment
CSP	Cloud Service Provider
FIM	Federated Identity Management
GC	Government of Canada
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
HSM	Hardware Security Module
IT	Information Technology
ITS	Information Technology Security
KEK	Key Encryption Key
MDM	Mobile Device Management
KMS	Key Management Service
MFA	Multi-Factor Authentication
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NVA	Network Virtual Appliance
SAML	Security Assertion Markup Language
SDN	Software Defined Network
SMB	Server Message Block
SSO	Single Sign-on
VM	Virtual Machine

6.2 GLOSSARY

Term	Definition
Cloud consumer organization	Any organization that wishes to acquire a CSP cloud service to implement a cloud-based service.
Configuration drift	Occurs when the configurations of production hardware and software differ from the backed up or recovery configurations.
Crypto erase	A sanitization process to erase the encryption key used on encrypted media to make the data unreadable.
Data residency	Data residency refers to the physical or geographical location of an organization's digital information while at rest.
Identity provider (IdP)	The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials.
Jump host	Also known as a jump server, a jump host offers controlled access between two dissimilar security zones.
Key encryption key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys to provide confidentiality protection.
Management plane	The element of a system that configures, monitors, and provides management, monitoring and configuration services to all layers of the system.
Multi-factor authentication	A characteristic of an authentication system or a token that uses two or more different authentication factors. The three types of authentication factors are something a user knows, something a user has, and something a user is.
Multi-tenancy	The allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.
OAuth	IETF standard for authorization that is very widely used for web services (including consumer services). OAuth is designed to work over HTTP.
On premises	Refers to the software and technology located within the physical confines of your organization.
Off premises	Refers to the software and technology located outside the physical confines of your organization.
OpenID	Standard for federated authentication that is very widely supported for web services. It is based on HTTP with URLs used to identify the identity provider and the user/identity (e.g. identity.identityprovider.com).
Sanitization	Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing. IT resources should be sanitized before they are released from classified information controls or released for use at a lower classification level.
Security assertion markup language (SAML)	OASIS standard for federated identity management (FIM) that supports both authentication and authorization. It uses XML to make assertions between an identity provider and a relying party. Assertions can contain authentication statements, attribute statements, and authorization decision statements.
Storage availability	System uptime of storage service, i.e. the storage system is operational and can deliver data upon request. Historically, this has been achieved through hardware redundancy.
Storage durability	Refers to long-term data protection, i.e. the stored data does not suffer from bit rot, degradation or other corruption. Rather than focusing on hardware redundancy, it is concerned with data redundancy so that data is never lost or compromised.

Term	Definition
Workload	A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction.

6.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management.* March 2019.
2	Canadian Centre for Cyber Security. *ITSP.50.103 Guidance on Security Categorization of Cloud-Based Services.* N.D.
3	National Institute of Standards and Technology. *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing*. December 2011.
4	National Institute of Standards and Technology. *Special Publication 500-292, Cloud computing reference architecture*. September 2011.
5	Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. 2017.
6	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach.* November 2012.
7	National Institute of Standards and Technology. *Special Publication 800-145, The NIST Definition of Cloud Computing.* September 2011.
8	Cloud Standard Customer Council. *Practical Guide to Hybrid Computing V3.0*. 2017.
9	Office of the Privacy Commissioner of Canada. *Cloud Computing for Small and Medium-sized Enterprises*. June 2012.
10	Treasury Board of Canada Secretariat. *Cloud Security Risk Management Approach and Procedures*. 2018.
11	Canadian Centre for Cyber Security. *ITSM.50.100 Cloud Service Provider Information Technology Security Assessment Process.* October 2018.
12	National Institute of Standards and Technology. *Special Publication 800-146, Cloud Computing Synopsis and Recommendations*. May 2012.
13	Canadian Centre for Cyber Security. *ITSP.50.106 Guidance on Cloud Service Cryptography.* N.D.
14	National Institute of Standards and Technology. *Special Publication 800-88, Guidelines for Media Sanitization*. September 2006.
15	Canadian Centre for Cyber Security. *ITSP.40.006 V2 IT Media Sanitization*. July 2017.
16	Canadian Centre for Cyber Security. *ITSP.30.031 V2 User authentication guidance for information technology systems*. August 2016.
17	National Institute of Standards and Technology. *Special Publication 800-63-3, Digital Identity Guidelines*. June 2017.
18	National Institute of Standards and Technology. *Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. January 2014.