National Cyber Security Centre

GUIDANCE

The NCSC is part of the Government Communications Security Bureau

July 2019

Cloud Computing: Shared Responsibility Security Models

Cloud computing is a general term describing networks of servers that house data, software applications, and services, and which are accessed via the Internet, rather than via on premise data centres. The US National Institute of Standards and Technology (NIST) defines cloud computing as:

> *... a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[1]

According to the NIST definition, the essential characteristics of cloud computing are:

- ***On-demand self-service*** – the Consumer can access computing capabilities as needed, without the need to interact with a customer service representative from the Provider's side
- ***Broad network access*** – the Consumer can access capabilities over the network, through standard mechanisms
- ***Resource pooling*** – the Provider's resources are pooled to serve multiple Consumers, with resources assigned according to Consumer demand
- ***Rapid elasticity*** – capabilities can be provisioned and released to scale rapidly in relation to Consumer demand
- ***Measured service*** – resource usage is monitored, controlled, and reported, which provides transparency for both the Provider and Consumer

[1] See NIST Special Publication 800-145, The NIST Definition of Cloud Computing, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

A variety of cloud service models are available to Consumers, each entailing different types of service management operation, as well as differing levels of responsibility for security for the parties involved. The three general service models discussed in relation to cloud computing are:

- Infrastructure as a Service (IaaS), where the Consumer does not manage or control the underlying cloud infrastructure infrastructure, but has control over operating systems, storage, and deployed applications, and possibly limited control over selected networking capabilities
- Platform as a Service (PaaS), where the Consumer does not manage or control the underlying infrastructure (including network, servers, operating systems, or storage), but has control over deployed applications
- Software as a Service (SaaS), where the Consumer does not manage or control the underlying cloud infrastructure or individual application capabilities

Cloud offerings, and the Service Level Agreements (SLAs) signed between Providers and Consumers, will vary in accordance with the services the Consumer selects from the Provider's offerings. In many cases, Providers offer "standard agreements" with common characteristics and costs. Organisations must be aware of the service levels they have agreed to with their Provider, and where possible tailor the SLA to their specific needs. A well-written SLA provides both the Consumer and the Provider with clarity and certainty regarding which party is responsible for what, in terms of security, performance, system availability, and service management. Further, an SLA must also specify the penalties and remedies the Provider will incur, should they not meet the agreed-upon service levels.

As noted above, the responsibility for security in a cloud environment differs depending on the service model adopted by the Consumer, and the extent to which the Consumer has migrated their systems into the cloud. Figure 1 provides a simplified understanding of differing responsibilities for security between the Provider and the Consumer, in relation to the extent to which the Consumer has migrated their systems into the cloud environment.

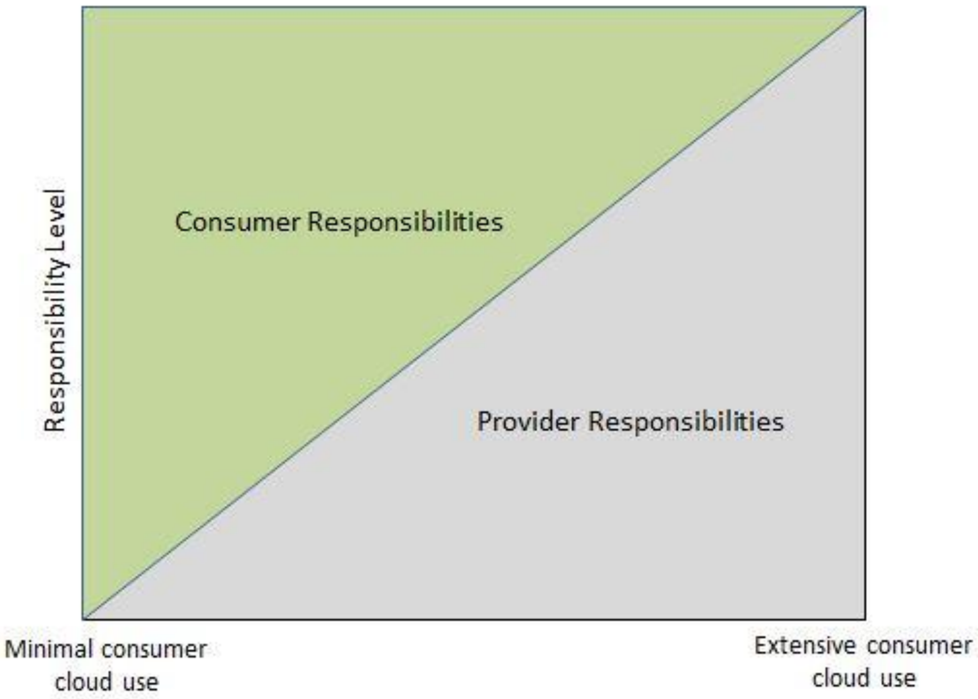

Responsibility Level
Consumer Responsibilities
Provider Responsibilities
Minimal consumer cloud use
Extensive consumer cloud use

Figure 1 – Differing responsibilities for security between the Provider and the Consumer

Figure 2 provides a simplified understanding of the differing levels of responsibility for security between the Provider and the Consumer, in relation to the cloud service model adopted by the Consumer. As indicated, the responsibility for security in an Infrastructure as a Service (IaaS) service model sees the responsibility for security rest mostly with the Consumer. In contrast, the responsibility for security in a Software as a Service (SaaS) service model sees the responsibility for security rest mostly with the Provider.

It is important that the Consumer of cloud services understand that, while certain responsibilities may rest with either Providers or Consumers, the ownership of any risk remains firmly with the Consumer. This overall ownership of risk should be distinguished from the management of specific risks, each of which may vary in type and magnitude.

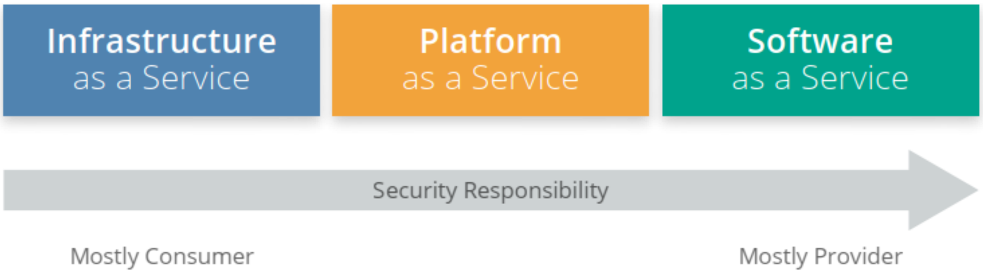
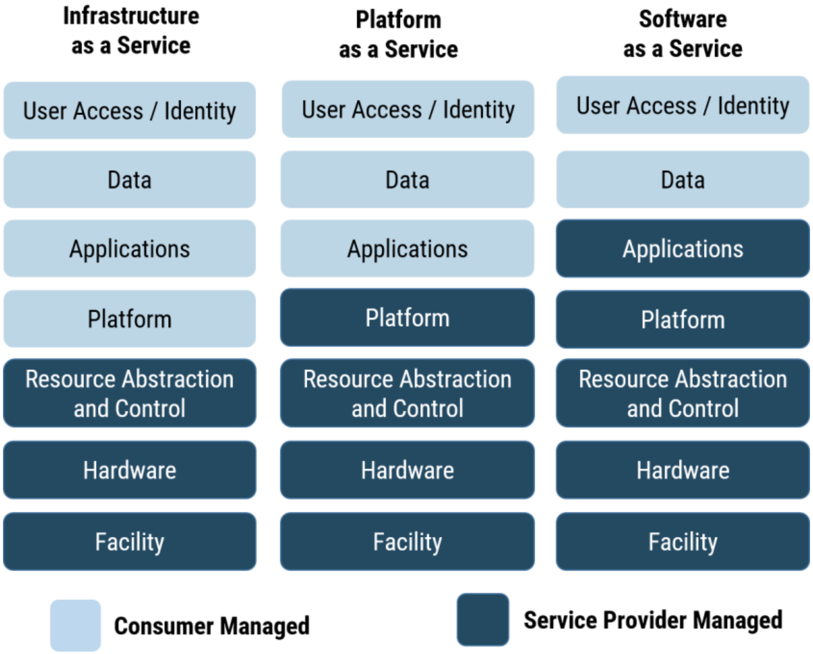


Figure 2: Cloud Security Alliance Security Guidance v4 – Security Responsibility in Relation to Cloud Service Model

Figure 3 provides more granular detail on where the security responsibilities for particular functions likely fall, depending on the model adopted by the Consumer.



Infrastructure as a Service	Platform as a Service	Software as a Service
□ User Access / Identity	□ User Access / Identity	□ User Access / Identity
□ Data	□ Data	□ Data
□ Applications	□ Applications	■ Applications
□ Platform	■ Platform	■ Platform
■ Resource Abstraction and Control	■ Resource Abstraction and Control	■ Resource Abstraction and Control
■ Hardware	■ Hardware	■ Hardware
■ Facility	■ Facility	■ Facility

□ Consumer Managed ■ Service Provider Managed

Figure 3: Government of Canada: Cloud Computing Shared Security Responsibility Model

The simplified models provided in this document are of most value when discussing cloud computing in general terms.

Once the responsibilities involved in adopting a particular cloud service model are clear, it becomes easier to focus any follow-up questions around the management of risk. Assurance is a critical component of risk management, particularly when the routine responsibility for specific services, applications, platforms and/or infrastructure rests with the Provider, rather than the Consumer. Accountability for malware detection, physical security, application and operating system patching, system maintenance, and data management are just some of the areas that must be well understood by all parties involved. Acceptable means to demonstrate assurance and monitor security must be agreed upon by the Consumer and the Provider, along with the means by which parties are held to account to the requirements set out in the Service Level Agreement.

Chapter 2.3 of the New Zealand Information Security Manual (NZISM) provides references to the mandatory controls associated with cloud services, as well as to further advisory content, in relation to information security requirements within the New Zealand Government.2 When considering cloud service models, organisations should also reflect on any other relevant obligations they may have. These may include legislative requirements under the Privacy Act 1993, the Public Records Act 2005, and the Official Information Act 1982.

The Government Chief Digital Officer (GCDO) also offers a range of advice on cloud computing for New Zealand Government agencies3. Guidance provided by GCDO includes:

- Developing and implementing a cloud plan https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/develop-and-implement-a-cloud-plan/
- Assessing the risks of cloud services https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/
- Designing for and implementing security controls for cloud services https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/design-for-and-implement-security-control-for-cloud-services/, and
- Frequently asked questions related to cloud risk assessments https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/additional-background-information/frequently-asked-questions-cloud-risk-assessment/

References

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, https://www.cloudsecurityalliance.org/artifacts/security-guidance-v4/

Government Chief Digital Officer, New Zealand Department of Internal Affairs, https://www.ict.govt.nz

Government Communications Security Bureau, New Zealand Information Security Manual, https://www.nzism.gcsb.govt.nz/ism-document/

Cloud Security Risk Management (ITSM.50.062) https://cyber.gc.ca/en/guidance/cloud-security-risk-management-itsm50062

NIST Cloud Computing Reference Architecture SP 500-292, https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

NIST Definition of Cloud Computing SP 800-145, https://csrc.nist.gov/publications/detail/sp/800-145/final

NIST Guidelines on Security and Privacy in Public Cloud Computing SP 800-144, https://csrc.nist.gov/publications/detail/sp/800-144/final

[2] Government Communication Security Bureau (GCSB), New Zealand Information Security Manual, Information Security within Government – Approach to Cloud Services, https://www.nzism.gcsb.govt.nz/ism-document/#226

[3] New Zealand Government Chief Digital Officer (GCDO), https://www.ict.govt.nz