National Cyber Security Centre

GUIDANCE

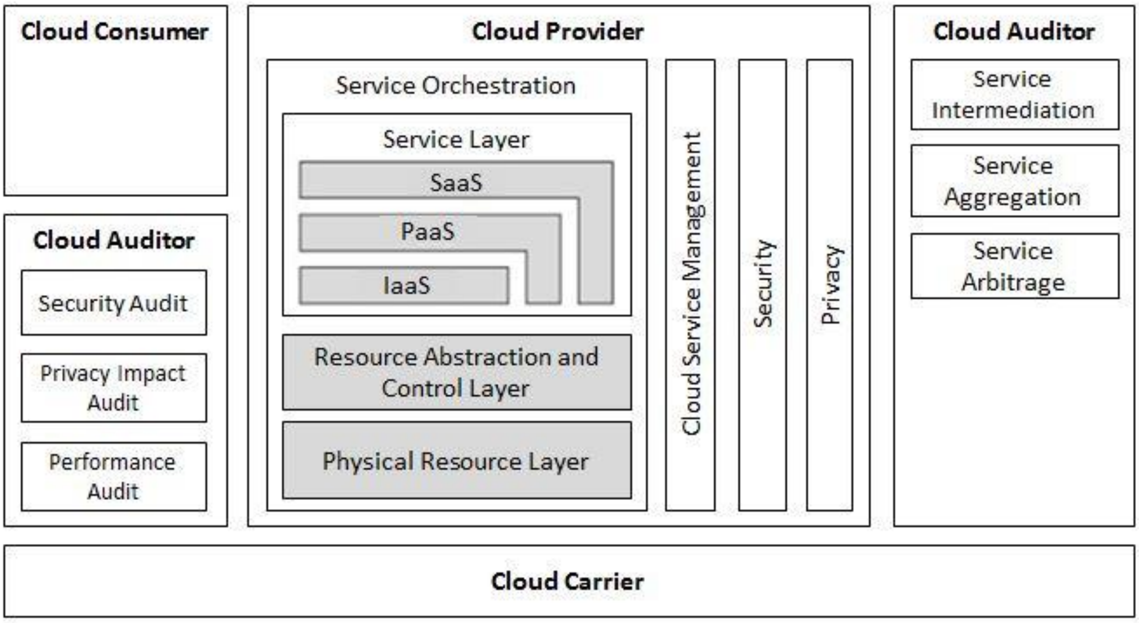
The NCSC is part of the Government Communications Security Bureau

July 2019

Cloud Services: Who's Who – Roles and Responsibilities

The move to cloud computing is occurring rapidly. Its adoption presents organisations with significant potential benefits in relation to costs, utility, scalability, security, and disaster recovery. It also represents a shift in the way organisations manage their ICT and who they partner with. Understanding the different possible roles involved in cloud computing, their respective responsibilities, and how they interrelate, will be helpful for organisations using cloud services.

The US National Institute of Standards and Technology (NIST) provides a useful graphic identifying these different roles.

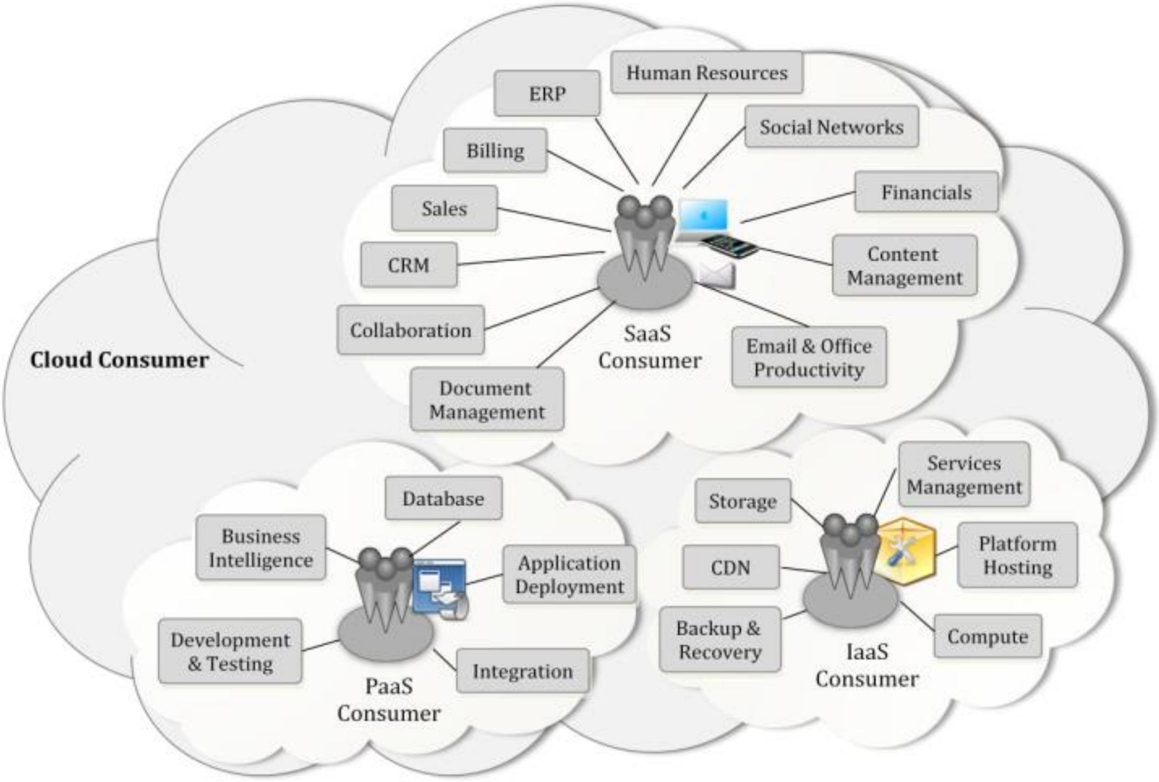


NIST SP 500-292 Cloud Computing Security Reference Architecture Approach

1. Cloud Consumer

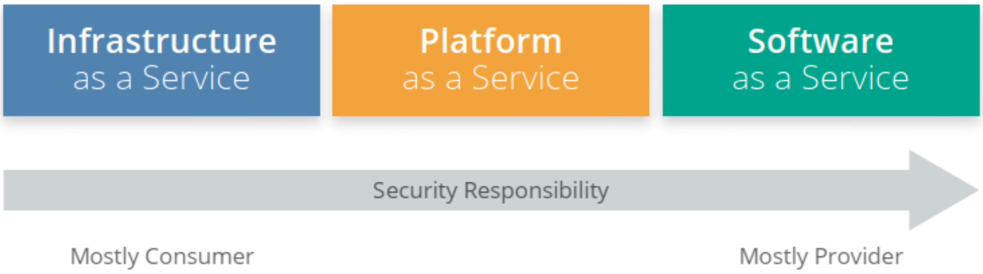
A Cloud Consumer is that person, organisation, or entity that has a business relationship with a Cloud Provider, using the Provider's services and products. For our purposes, Cloud Consumers are the Government Departments, Agencies, and other organisations (including those in the private sector) who have made, or are looking to make, the move to the cloud computing model.

The Cloud Consumer has the choice from a number of cloud service models (Infrastructure as a Service, Platform as a Service, Software as a Service), depending upon their specific requirements.



NIST SP 500-292 Example of Services Available to a Cloud Consumer

The responsibilities for the security requirements of each of these models, in relation to the Cloud Consumer and the Cloud Provider, vary depending upon the model adopted by the Consumer. The technical requirements a Consumer requires of its Provider must be specified in a Service Level Agreement (SLA) between the two parties.

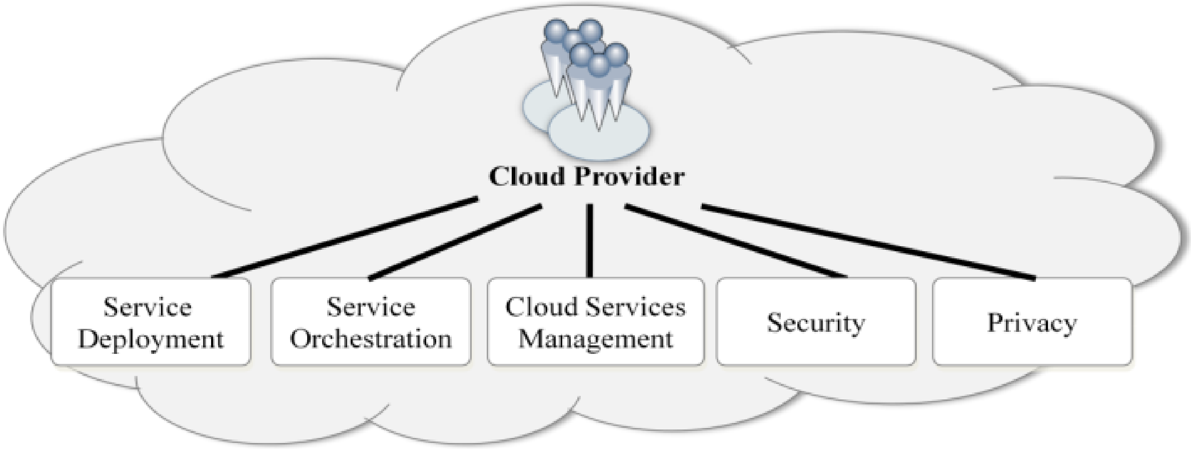


Cloud Security Alliance Security Guidance v4 – Security Responsibility in Relation to Cloud Service Model

2. Cloud Provider

Cloud Providers are the entities that make cloud services available to Consumers. They may or may not own the infrastructure. There are three broad types of cloud service available: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Decisions around the consumption of services are based upon the needs of the consumer, and their Governance, Risk and Compliance (GRC) settings.

A Cloud Provider conducts activities in five main areas: service deployment, service orchestration, cloud services management, security, and privacy.



NIST SP 500-292 Cloud Provider – Major Activities

3. Cloud Carrier

A Cloud Carrier is the intermediary that provides the connectivity and transport of cloud services between Consumers and Providers, via access devices such as network and telecommunications technologies. The technical capacity of Carriers may affect the bandwidth through which Consumers can access information and applications hosted in the cloud. Whilst the processing abilities of a Cloud Provider's data centre may be significant, network bottlenecks may impact the performance experienced by the Consumer. Latency, bandwidth, and the resulting impacts on speed of delivery, are considerations in the provision of cloud services to the Consumer.

4. Cloud Broker

Cloud Brokers have emerged because of the increasing complexity of the cloud computing environment. A Cloud Broker is an entity that manages the use, performance, and delivery of cloud services, and that negotiates relationships between Providers and Consumers. They exist to simplify and enhance the Cloud Consumer experience. In general, Cloud Brokers offer a variety of services, which fall into three categories:

- ***Service Intermediation***, where the Broker enhances a service by improving capability and providing value-added services to the Consumer
- ***Service Aggregation***, where the Broker combines and integrates services into new services, provides data integration, and ensures the secure movement of data between the Consumer and their Providers
- ***Service Arbitrage***, where the Broker has the flexibility to choose services for the Consumer from multiple Providers

As with any market, Cloud Brokers differ in their levels of independence and reliability. Some companies appear to offer "brokerage" services, but may be on-selling suites of existing products.

Fee structures and the "value add" offered by each Broker will differ on a case-to-case basis. Any organisation looking to make use of Cloud Brokerage services should develop an understanding of the options available to them, and the strengths and weaknesses of these options, before making any decision.

5. Cloud Auditor

As organisations look to move to the cloud, both Consumers and Providers need ongoing assurance that there are controls in place that provide the security, privacy, and performance required of the services purchased by the Consumer. Cloud Auditors perform independent examinations of cloud services, in order to confirm these controls meet the required standards. Audits identify strengths, vulnerabilities, and areas where performance improvements might be achieved.

Audits often look at the operational effectiveness of systems, data, security, and risk management. They can also focus on system monitoring, logical and physical access, change management, and administrative and organisational structures and practices. The areas that an Auditor will focus on, and the nature of the reporting they provide, will differ according to type of audit being conducted, and on the agreed scope of the activity.

6. Cloud Access Security Broker (CASB)

Cloud Access Security Brokers (CASBs) are a form of Security as a Service (SECaaS) provider, which offer the Consumer security policy enforcement points that sit between the end-users and the Providers. At a minimum, a CASB should:

- provide an organisation visibility into cloud use across the organisation,
- ensure and demonstrate an organisation's compliance with regulatory requirements,
- provide a way for an organisation to ensure data stored in the cloud is secure, and
- provide a degree of threat protection that ensures any risks incurred by an organisation operating in the cloud is at an acceptable level

As with any commercial arrangement, the extent of the services a CASB offers, and the reach it has into agency data, should be clearly expressed in the SLAs signed between the Consumer and the CASB. Organisations must have a clear understanding of both what is, and what is not, covered in an SLA.

References

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

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