
## Some Cloud Basics

In September 2011, the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce recommendation regarding the definition of cloud computing assisted the states' identification and categorization of the various cloud computing models and, theoretically, the development of the sales tax policies addressing those models.

The NIST defines cloud computing as a model for enabling –

- ubiquitous (present, appearing, or found everywhere, omnipresent, ever-present, everywhere, universal, pervasive, worldwide, global),
- convenient,
- on-demand network access

to a shared pool of configurable computing resources (for example, **networks**, **servers**, **storage**, **applications** and **services**) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST is only one in a veritable sea of global standards bodies proposing guidelines and frameworks. Along with PCI-DSS, SOX, HIPAA, and international laws that mandate specific cybersecurity requirements, standards from NIST, ISO/IEC (27000 series), CobiT, and COSO. The NIST further provides that the cloud model is composed of five essential characteristics, three service models, and four deployment models. The three service models are particularly relevant to states sales tax, especially considering the opportunity to structure a contract as the provision of a nontaxable service in a specific state rather than as a taxable service or sale of software in another state.

The NIST defines the following three cloud computing service models, each with unique applications to different businesses and users:

- ***Software-as-a-Services (SaaS)***
    - The capability provided to the consumer is to use the CSP'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.
    - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
    - The SaaS model is utilized by individual users and businesses desiring lower-cost alternatives to traditional licensed software.
- ***Platform-as-a-Service (PaaS)***
    - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the CSP.
    - The consumer does not manage or control the underlying cloud infrastructure, including network, services, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
    - The PaaS model is typically utilized by programmers, developers, and web designers.
- ***Infrastructure-as-a-Services (IaaS)***
    - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.


- The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly, limited control of select networking components (for example, host firewalls).
- The IaaS model typically applies to large corporations that have the internal capability of maintaining complete control over their data.

Each model has unique characteristics that will drive a state's imposition of sales tax on the related charges, specifically when a state is determining whether the charges relate to the determination that a transaction pertains to tangible personal property or a service. For example, a state may categorize the SaaS model as entirely a service, but the IaaS model as either a service (purchases from the cloud computing provider) and tangible personal property (licensing of third party software installed on the cloud devices) or entirely tangible personal property (licensing of software and rental of hardware).

NIST's Special Publication 800 series reports on the research, guidance and outreach efforts of NIST's Information Technology Laboratory (ITL) in computer security and its collaborative activities with industry, government, and academic organizations. While NIST standards documents have direct applicability to U.S. Federal government information security practices, they have also become de facto standards for information security best practices.

Arguably, the risks of inappropriate disclosure or data breach and selection of third party providers into the cloud services are largely, if not entirely, in the CSPs control. Therefore, making the CSP responsible for these risks seem appropriate.

**Service Levels and Service Credits**

Cloud service customers need to determine their requirements and objectives for a given cloud service to be able to match their requirements to a CSP's capabilities.

How is this accomplished?

- Well, for starters, prior to beginning the cloud procurement process, it is important for the customer to determine its minimum requirements for the cloud service (including requirements for reliable performance, timely access, data integrity and security).
- These minimum requirements should then be used by the customer during the procurement process to identify CSPs capable of satisfying the customer's requirements.
- The metrics used by the CSP and customer to measure compliance with the customer's requirements are typically found in the service level agreement (SLA).

More to come . . .