ADVANCED CONSULTING PARTNER
AUTHORIZED GOVERNMENT PARTNER
CHANNEL RESELLER PARTNER

Procurement Guide: Understanding Amazon Web Services

Written by Chris Rader, Contracts Administrator

The dynamic nature of cloud computing can often present a challenge for procurement professionals, as traditional practices and contracting vehicles were designed to help IT mangers provision hardware and software, not on-demand services like the cloud. However, procuring the Amazon Web Services (AWS) cloud doesn't have to be as problematic as it appears to be. Gaining an understanding of how the technology drives the "terms and conditions" simply requires a new frame of mind.

Every contract has the same basic elements that make it a contract – offer and acceptance, consideration, and the intention to be legally bound – and what legal language is crafted to capture the risks is driven by the nature of the purchase. For example, a construction contract is much different than a telephony contract, which is much different than a software-as-a-service contract.

To help your agency or organization navigate the AWS cloud procurement model, DLT Solutions has developed this helpful guide. It explores what a contract is for AWS, who owns what in the AWS environment, available solutions for the AWS platform, and more. Read on to gain answers to some of your most common questions…

What is a contract for AWS?

If you have ever rented a data center or purchased a utility service, you are already familiar with many of the concepts we will cover in this guide. If you have not put a contract in place for either, grab a coffee and get ready for a top-level view of something that is likely very new to your agency or organization.

Let's start with a concept that is easy to understand and difficult to craft language around: *responsibility*. Your agency is responsible for what you control and AWS is responsible for what it controls.

Seems fair, but **what exactly is it that you control?**

At a high level, AWS controls everything up to the hypervisor . This includes physical security of the data center where your information is stored and a myriad of process and systems to manage the backend security, compute power, data storage and the electricity to power and cool the systems. Your agency or organization is responsible for everything *above* the hypervisor. This includes managing applications, configuring the security group firewall and more. An in-depth explanation of this shared security model can be found in the Amazon Web Services: Overview of Security Processes white paper.

So who owns what within the AWS environment?

AWS owns everything it controls, and you own everything you control. The way the contract is written, AWS claims no right to your data and gives you no rights to the data it uses to run its data centers. There is an analogy I like to describe this. For those of us who are responsible for a water bill, we know that the water utility company is responsible for providing a constant stream of safe portable water. The water utility company is responsible for the security of the water sanitization facility, removing dangers from the water, adding beneficial components to the water, and for delivering the water through their pipes to your pipes. Once the water reaches your pipes, complete responsibility for the water is transferred from the water utility to you. You are responsible for the pipes that you control and the usage of the water coming out of the pipes. The water utility does not encroach on your rights and does not tell you what to do with the water. You can water your lawn, make dinner, give water to the neighbors, or create an ice sculpture of the King of Pop. The water utility does not care what you do with the water (and won't judge you for it), they just want to get paid for what you choose to use.

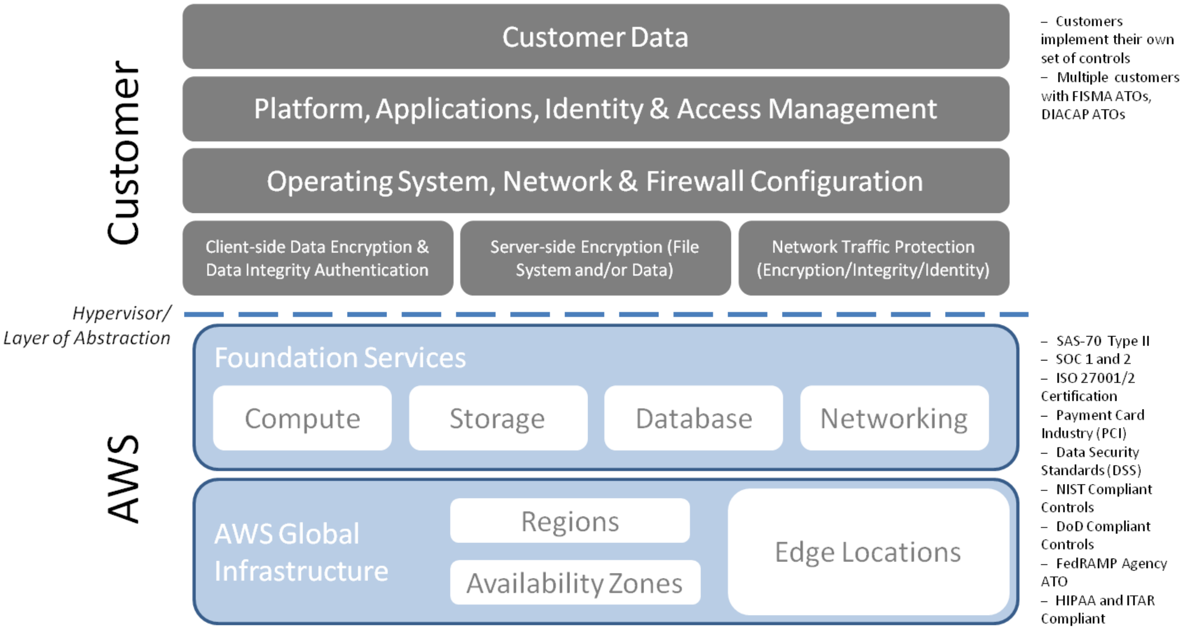
Customer
Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption/Integrity/Identity)
– Customers implement their own set of controls
– Multiple customers with FISMA ATOs, DIACAP ATOs
Hypervisor/ Layer of Abstraction
AWS
Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
– SAS-70 Type II
– SOC 1 and 2
– ISO 27001/2 Certification
– Payment Card Industry (PCI)
– Data Security Standards (DSS)
– NIST Compliant Controls
– DoD Compliant Controls
– FedRAMP Agency ATO
– HIPAA and ITAR Compliant

Figure 1 – This diagram explains the division of responsibility and control. AWS is responsible for everything below the layer of abstraction/hypervisor, and you, as the customer, are responsible for everything above.

What can you do in AWS?

The possibilities are almost endless – you can do just about anything you can do with a computer, as long as it is not an attack on AWS or others, or is illegal. AWS is being used today to run complex computations to find the cure for cancer, host blogs and websites, as well as run multinational webbased businesses such a Netflix. And yes, Amazon.com does run on AWS. To see more examples of how agencies and organizations are using the AWS platform, visit www.dlt.com/awsinaction.

What is AWS doing to keep data safe?

With governments hacking, leakers leaking and bored teenagers on the prowl— data security has never been more prominent in the news. AWS provides security for what it controls, up to the hypervisor. *Security for what you control must be architected by your team*. However, AWS and their partners can provide your agency or organization with security architecture support, as well as provide guidance on the best available tools to help you customize your security controls, procedures, and protocols.

Does AWS have access to my data?

You might be surprised, but the answer is no. Your agency or organization's coders are able to access the code that AWS uses to manage their data centers and the software that helps run them, but AWS does not have access to your passwords or data. AWS cannot mine your data. It is important to note, however, that AWS does not operate entirely in the dark. AWS has developed tools that let them track usage. For example, AWS can see that you moved 10 gigabytes of data from a server you control into Glacier (an AWS storage service), but they have no idea what makes up the 10 gigabytes of information. AWS can see when you are trying to access your information, and they can also see if someone else is trying to access your information. This is an important element that helps AWS safeguard your information and stave off attacks from hackers and other malicious organizations.

What if my organization manages data that is governed by statutes like HIPAA?

AWS provides what is needed to comply with HIPAA and other statutes from the hypervisor down. It is up to your agency or organization to architect a solution *above the hypervisor* that is compliant with the requirements of the subject regulation (keep in mind, there are companies out there that can assist your agency or organization in architecting this framework). If it is necessary to have AWS certify that they comply with HIPAA, they can provide documentation that verifies they meet the requirements from the hypervisor down.

Should you architect a solution above the hypervisor that fits within the parameters of these regulations; AWS will sign their documentation with a caveat. It is important to note that in order for AWS to comply with audit and security provisions, your agency or organization can only put HIPAA and other sensitive data in certain places in AWS, in certain configurations.

If your organization manages HIPAA or other sensitive data and does not want to be limited to the AWS restrictions, you may still architect that solution, but certain steps need to be followed. For more information on how you can create systems on AWS that comply with HIPAA, check out the Creating Healthcare Data Applications to Promote HIPAA and HITECH Compliance white paper. **Why do it this way?** Most HIPAA regulations speak to things that happen above the hypervisor level. Since AWS does not have access to or control over that data, it carves out its responsibility only for the things that it controls. Should your organization decide that it does not want to manage HIPAA data in AWS, then hiring a third party to perform these managed services would be the best route. A cloud managed services provider can architect the solution, implement the necessary protocols and procedures, and take on the risk managing your PHI within the constraints of that contract.

In conclusion…

The AWS cloud is very flexible, very powerful and very different than software-as-a-service or cloud managed services. If after you review the platform you find that AWS does not meet the needs of your organization, we encourage you to take another look. It is likely that AWS does in fact meet or exceed the requirements for your organization – from the hypervisor down. For applications and systems above the hypervisor, policies and procedures for running your organization's data centers (if applicable) will need to be tailored and applied to running in the cloud. Another approach would be to have a cloud managed services provider, such a DLT Solutions, administer your AWS environment on your behalf and at your direction.

Contact Information

For additional questions about AWS and the cloud procurement model, please contact us:

The DLT Cloud Advisory Group
1-855-CLOUD01 (256-8301)
cloud-solutions@dlt.com
www.dlt.com/cloud
#DLTCloud