Security and Compliance OF the Cloud vs. Security and Compliance IN the Cloud

April 19, 2016

Kevin Tam, Managing Director
Agenda

- Introduction
- Compliance FAQs for Cloud Service Providers
- Cloud – Definition
- Cloud – Industry Overview
- Security and Compliance OF the Cloud
  - What’s In Place Today?
  - Compliance is Not One-Size Fits All
- Security and Compliance IN the Cloud
  - Customer Responsibility
- So, What’s the Answer?
- Questions
Introduction

- Independent cybersecurity services company
  - Assessment and advisory
  - Technical testing
  - Compliance management technology solutions

- Founded in 2001, offices throughout the US and UK

- About me:
  - Managing Director, Northwest
  - Leads our Technology Assessment and Advisory Services (TAAS) team
  - Joined in 2014
  - Prior to Coalfire, 11+ years with Big 4, two years building out Risk and Compliance practice
Compliance FAQs for Cloud Service Providers

- How does leveraging [name of CSP] make my security and compliance activities easier?
- Now that we are in the cloud, how do we configure our environment to be [name of compliance standard] compliant?
- I see that [name of CSP] is [name of compliance standard] compliant, does that mean if we leverage their services we will be compliant as well?
- If [name of CSP] is non-compliant, how does that impact my compliance?
Cloud – Definition

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

NIST definition of cloud computing:
Cloud – Industry Overview

$160 Billion Cloud Market by 2020

Trends for growth:
Accelerating Adoption – Efficiencies (operational, financial), rapid scalability, visibility into data and security.

57% of North American and European enterprise infrastructure decision-makers considered use of public cloud a high or critical priority in the next 12 months.¹

¹ Forrester: Understanding the Cloud Services Provider Landscape
Security and Compliance OF the Cloud

- Security and compliance OF the cloud refers to how the Cloud Service Provider manages the security and compliance of the cloud environment.
- Typically, the CSP manages the underlying infrastructure and associated controls.
- Depending on the type of service and the offerings utilized by the customer, additional controls can also be the responsibility of the CSP or be a shared responsibility between the CSP and the customer.

How are CSPs demonstrating that they have controls in place?
How do customers know what controls are their responsibility?
How can a customer trust their CSP?
Compliance is Not One-Size Fits All

Various Compliance Frameworks / Certifications

- PCI
- ISO/IEC 27001
- HIPAA/HITECH
- FedRAMP
- AICPA SOC 2
What’s In Place Today?

Microsoft Azure Trust Center

The trusted cloud

- Security and privacy are embedded into the development of Azure
- Security: We work to keep your data safe
- Privacy: You own and control your customer data
- Transparency: You know how your data is stored and accessed, and how we help secure it
- Compliance: We conform to global standards

Microsoft understands that for you—our enterprise customer—to realize the benefits of the cloud, you must be willing to entrust your cloud provider with one of your most valuable assets—your data. If you invest in a cloud service, you must be able to trust that your customer data is safe, that the privacy of your data is protected, and that you retain ownership of and control over your data—that will only be used in a way that is consistent with your expectations.

Microsoft strives to earn your trust in Microsoft Azure. Our long experience running online services has involved extensive investment in foundational technology that builds security and privacy into the development process. Over time, we’ve developed industry-leading security measures and privacy policies, and participated in international compliance programs with independent verification of how we measure up.

Independent Audits of Infrastructure, Services, and Operations

Our customers and regulators expect independent verification of security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations.

Google has annual audits for the following standards:

- PCI
- HIPAA
- EU Data Protection Directive
- Resources
- Security
Security and Compliance *IN* the Cloud

- Security and compliance *IN* the cloud refers to the responsibilities associated with a customer for their security and controls.

- What these specific responsibilities are depends on a number of factors:
  - Cloud service model (e.g., IAAS, PAAS, SAAS)
  - Cloud service offerings being utilized
  - Relevant and applicable compliance certifications and frameworks

- Controls can be the responsibility of the CSP, the customer, or shared

How do I determine my specific responsibilities as a customer?

How do I ensure I’m taking full advantage of the Cloud for my security and compliance needs?
Customer Responsibility

1. Have a clear understanding of your compliance requirements

2. Have a clear understanding of your compliance scope definition

3. Perform a risk assessment

4. Work with your CSP to determine / identify key control responsibilities (i.e., CSP, customer, or shared responsibility)

5. Perform vendor risk management
So, What’s the Answer?

- How does leveraging [name of CSP] make my security and compliance activities easier?
- Now that we are in the cloud, how do we configure our environment to be [name of compliance standard] compliant?
- I see that [name of CSP] is [name of compliance standard] compliant, does that mean if we leverage their services we will be compliant as well?
- If [name of CSP] is non-compliant, how does that impact my compliance?
Q&A

Contact Information
Kevin Tam, Managing Director - NW
kevin.tam@Coalfire.com
206.352.6028 x7595