Chapter 7
Security and Compliance:
IaaS, PaaS, and Hybrid Cloud

Heather Hinton
IBM Corporation, USA

ABSTRACT

Despite a rocky start in terms of perceived security, cloud adoption continues to grow. Users are more comfortable with the notion that cloud can be secure but there is still a lack of understanding of what changes when moving to cloud, how to secure a cloud environment, and most importantly, how to demonstrate compliance of these cloud environment for regulatory purposes. This chapter reviews the basics of cloud security and compliance, including the split of security responsibility across Cloud provider and Client, considerations for the integration of cloud deployed workloads with on-premises systems and most importantly, how to demonstrate compliance with existing internal policies and workload required regulatory standards.

INTRODUCTION

Despite a rocky start in terms of perceived security, cloud adoption continues to grow. Users are growing more comfortable with the notion that cloud can be secure. A recent study by the Economist Intelligence Unit found that "the most mature enterprises are now turning to cloud strategies as a strategic platform for growing client demand and expanding sales." (Columbus, 2015; Economist Intelligence Unit, 2015). While initial fears of would-be-cloud-adopters focused on the security of the Cloud provider's environment, most analysts have now moved beyond that to focus on governance of the client's cloud-hosted workload.

Charting the change in viewpoint, in 2013, typical articles all cited cloud as insecure and not safe for data and workloads:

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology

DOI: 10.4018/978-1-5225-5634-3.ch007

advances, so do the risks that come with adopting them…"The cloud is not for everyone," [Neil] Rerup said. "Like with all solutions, you have to weigh what level of risk you are comfortable dealing with." (Angeles, 2013)

By late 2014, the overall tone was changing to recognize that while breaches will still occur when using cloud, it is not going to be the cloud provider's fault:

Cloud data breaches are a sure thing. Forrester doesn't mince words with this one, saying that CIOs should expect to encounter a breach in the cloud – and that it will be their fault, not the SaaS provider. "The culprits will likely be common process and governance failures such as poor key management or lack of training or perimeter-based thinking by your security department," the report states. (Gagliordi, 2014)

And by 2015, analysts such as Jay Heiser of Gartner, were articulating the need for clients to move beyond security and embrace oversight and governance, in particular for the client's own use of the cloud:

The ongoing concern about cloud 'security' is distracting from what is ultimately the more significant concern "how are you going to ensure that your employees make appropriate, safe and secure use of applications that you are not running in house?" The biggest 'security' problem isn't that SaaS vendors are being hacked, its that your users are putting sensitive data into SaaS without recognizing that they need to control access and usage. Its time for the cloud risk community to evolve beyond superficial concepts of 'cloud security' and start strategizing 'cloud governance' approaches. (Heiser, 2015)

Despite this encouraging move to cloud, and the need for cloud governance, there is still a lack of understanding of what changes when moving to cloud, how to secure a cloud environment, and most important, how to demonstrate compliance of these cloud environment for regulatory purposes. This chapter introduces the basics of understanding the roles and responsibilities for Cloud security, how to secure a cloud-hosted workload, how to integrate this with in-house, or on premises systems, and most importantly, how to approach governance through compliance with existing internal policies and workload required regulatory standards.

BACKGROUND

IaaS – Infrastructure as a Service - is the most basic of Cloud offerings. IaaS platforms provide physical and virtual servers in a consumptive, on-demand manner. These resources are deployed by the provider's orchestration and automation tools; they use the provider's network infrastructure to interconnect the servers to each other and to the Internet and/or the client's internal, on-premises network. IaaS services are typically "self-serve" where the client has complete control over their deployed environment. Well-known IaaS providers include Amazon Web Services (AWS), Microsoft Azure, Google, and IBM SoftLayer. Some providers also include a "managed services" option, by which the provider will handle the operational management (configuring, maintaining) of a cloud environment, such as with IBM's Managed Services for Cloud.