Compliance and the Cloud: What You Can and What You Can’t Outsource

Presented By:

Kate Donofrio
Security Assessor
Fortrex Technologies
Agenda

- Instructor Biography
- Background On Fortrex
- What’s In A Cloud?
- Pick A Cloud
- Draft NIST SP800-146 Considerations
- PCI DSS Scope
- PCI SSC Guidance
- Sample Cloud Provider Stances
- CSA Cloud Controls Matrix
- Outsource Considerations
Background on Fortrex

General Facts

- IT Security, Operational Risk and Advisory Services
- Founded in 1997
- Headquarters in Frederick, Maryland
- Privately Held
- Approaching 1,000 Customers
  - Baltimore to Alaska to Guam
- Broad Industry Coverage
- QSA, PA-QSA & ASV
- Abundance of References

Integrity, Excellence, Empowerment, Teamwork and Thankfulness
What’s In A Cloud?

• NIST Special Publication 800-146 defines a “cloud” as a service which:
  ○ Maintains a pool of hardware resources to maximize service, minimize cost
  ○ Resource efficiency permits hardware refresh, migration of customer workloads
Pick A Cloud: History of the Cloud

• 1950s Mainframes
  o Client/Server Model
  o “Time-Sharing”

• 1960s
  o “Intergalactic Computer Network”
    ▪ J.C.R Licklider – ARPANET
  o “Computation being delivered as a public utility”
    ▪ John McCarthy - 1961

• 1999 Salesforce.com
  o Applications over the internet

• 2006 Amazon EC2 – Rent technology

• 2009 Web 2.0 – Browser based applications
Pick A Cloud: Private

- Centralized or distributed
- Dedicated to single entity
- Examples may include Data Warehouses or co-located cardholder data environments
Pick A Cloud: Community

- Provide and/or subscribe
  - At least one participant must provide a service
- May include one or many entities
- Examples may include Wikipedia or SharePoint site structures
Pick A Cloud: Public

- Potentially large computing and storage resources afford clients elasticity
- Communication links are generally provided over the public Internet
- Serves a diverse pool of clients
- Workload locations are hidden from clients
- Limited visibility and control over data security
- Examples may include Amazon or RackSpace
Pick A Cloud: Hybrid

- Composed of two or more private, community, and/or public clouds

- Uses may include “Cloud bursting” – client employs private cloud and accesses one or more public clouds during periods of high demand

- May serve as backup resource
  - Disaster recovery
Pick A Cloud: Environments

- **Software as a Service (SaaS)** – Application access and use
  - Google, Twitter, Facebook

- **Platform as a Service (PaaS)** – Access to tools and execution resources to develop, test, deploy and administer applications
  - Operating Systems, Network Access, Hosting, Database Management

- **Infrastructure as a Service (IaaS)** - Access to virtual computers, network-accessible storage, network infrastructure components such as firewalls, and configuration services
NIST SP800-140 Considerations

• Off-line Data Synchronization
• Interoperability Between Cloud Providers
• Compliance
• Physical Location
• Support for Forensics
• Information Security Responsibilities
• Data Privacy
PCI DSS Scope

To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

• The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that **no cardholder data exists outside of the currently defined cardholder data environment (CDE)**.

• Once **all locations of cardholder data** are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).

• The entity considers **any cardholder data found to be in scope** of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.

• The entity **retains documentation that shows how PCI DSS scope was confirmed and the results**, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.
June 2011 PCI DSS Virtualization Guidelines state:

• Perform a detailed assessment of the unique risks associated with each service

• Hosted entity and provider clearly define and document the responsibilities assigned to each party for maintaining PCI DSS requirements and any other controls that could impact the security of cardholder data.

• Cloud provider should clearly identify which PCI DSS requirements, system components, and services are covered by the cloud provider’s PCI DSS compliance program and which are responsibility of the hosted entity

• Cloud provider should provide sufficient evidence and assurance that all processes and components under their control are PCI DSS compliant
PCI SSC Guidance

Define Responsibilities such as in the following example:

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Type of Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>IAAS</td>
</tr>
<tr>
<td>Software, user applications</td>
<td></td>
</tr>
<tr>
<td>Operating systems, databases</td>
<td></td>
</tr>
<tr>
<td>Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)</td>
<td></td>
</tr>
<tr>
<td>Computer and network hardware (processor, memory, storage, cabling, etc.)</td>
<td></td>
</tr>
<tr>
<td>Data center (physical facility)</td>
<td></td>
</tr>
</tbody>
</table>
PCI SSC Guidance: Public Cloud

• Distributed architectures add layers of technology and complexity
• Designed to be public-facing, to allow access into the environment from anywhere on the Internet
• Infrastructures are by nature dynamic, and boundaries between tenant environments can be fluid
• Hosted entities have limited or no visibility into the underlying infrastructure and related security controls
• Hosted entities have limited or no oversight or control over cardholder data storage
• Hosted entities have no knowledge of who they are sharing resources with, or the potential risks their hosted neighbors may be introducing to the host system, data stores, or other resources shared across a multi-tenant environment.

• Additional controls must be implemented to compensate for inherent risks and lack of visibility into architecture.

• These challenges **may make it impossible** for some cloud-based services to operate in a PCI DSS compliant manner.

• Evidence of cloud provider compliance should be subjected to rigorous review of controls.
Is AWS now PCI certified?
AWS provides a secure environment that has been validated by a QSA, allowing merchants to establish a secure cardholder environment and to achieve their own certification, having confidence that their underlying technology infrastructure is compliant.

What does this mean to me as a PCI merchant or service provider?
Our PCI Service Provider status means that customers who use our services to store, process or transmit cardholder data can rely on our PCI compliance validation for the technology infrastructure as they manage their own compliance and certification, including PCI audits and responses to incidents. Our service provider compliance covers all requirements as defined by PCI DSS for physical infrastructure service providers.
Does the PCI standard require single-tenant environments in order to be compliant?
No. The AWS environment is a virtualized, multi-tenant environment. AWS has effectively implemented security management processes, PCI controls, and other compensating controls that effectively and securely segregate each customer into its own protected environment.

Do QSAs for Level 1 merchants require a physical walkthrough of a service provider’s data center?
No. A merchant can obtain certification without a physical walkthrough of a service provider’s data center if the service provider is a Level 1 validated service provider (such as AWS). A merchant’s QSA can rely on the work performed by our QSA, which included an extensive review of the physical security of our data centers.
Sample Cloud Provider Stances: RackSpace

How do you handle payment for Cloud Sites™?
Cloud Sites is a multi-tenant hosted environment. The Payment Card Industry prohibits handling or maintaining credit card information in multi-tenant environments. Thus, all credit card processing must be handled completely by a third party payment gateway.

Building an e-commerce solution using Cloud Sites
Cloud Sites is designed to provide an elastic web-hosting environment. This capability can allow an e-commerce merchant to properly handle the high-volume shopping season without carrying extra infrastructure throughout the remainder of the year. Cloud Sites is not currently designed for the storage or archival of any credit card related information, all credit card information must be handled on the payment gateway.
Rackspace understands that organizations have different needs and requirements, especially when it comes to critical IT infrastructure. In support of this, Rackspace offers a portfolio of Private Cloud solutions.
Cloud Security Alliance
Cloud Security Matrix

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

The Cloud Security Alliance Cloud Controls Matrix (CCM) provides a controls framework in 13 domains aligned with industry-accepted security standards, regulations, and controls frameworks such as:

- ISO 27001/27002
- ISACA COBIT
- PCI DSS
- NIST
- BITS
- GAPP
- HIPAA/HITECH
- Jericho Forum
- NERC CIP
Cloud Security Alliance
Cloud Security Matrix

CCM domains include:

• Compliance
• Data Governance
• Facility Security
• Human Resource Security
• Information Security
• Legal

• Operations Management
• Risk Management
• Release Management
• Resiliency
• Security Architecture
Outsource Considerations

• What do you *really* need?

• What are you *really* getting?

• Do standards, regulatory, or framework compliance requirements impact planned service/system?

• Is the platform single or multi-tenant?

• Is the selected platform truly scalable?
Outsource Considerations

• What boundary controls are established?
• What security controls are enforced?
• How are information security responsibilities allocated?
• Does the provider support forensics?
• Where are utilized data center facilities? Are they accessible?
Questions?
Thank You.