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

Presented By:

Peter Spier
Managing Director PCI and Risk Assurance
Fortrex Technologies
• Instructor Biography
• Background On Fortrex
• What’s In A Cloud?
• Pick A Cloud
• NIST SP800-146 Considerations
• PCI DSS Scope
• PCI SSC Guidance
• Sample Cloud Provider Stances
• CSA Cloud Controls Matrix
• Outsource Considerations
Presenter Biography

- **Peter Spier** is Managing Director PCI and Risk Assurance at Fortrex Technologies ([www.fortrex.com](http://www.fortrex.com)) based in Frederick, Maryland.

- Certifications include: **CISSP, CRISC, CISM, PMP, QSA, PA-QSA, PCIP, and ITILFv3**

- Masters degree from Syracuse University School of Information Studies

- Over 15 years of experience
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
• 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:
  o Maintains a pool of hardware resources to maximize service, minimize cost
  o Resource efficiency permits hardware refresh, migration of customer workloads
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

- **Platform as a Service (PaaS)** – Access to tools and execution resources to develop, test, deploy and administer applications

- **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

February 2013 PCI DSS Cloud Computing Guidelines state:

The responsibilities delineated between the client and the Cloud Service Provider (CSP) for managing PCI DSS controls are influenced by a number of variables, including but not limited to:

- The purpose for which the client is using the cloud service
- The scope of PCI DSS requirements that the client is outsourcing to the CSP
- The services and system components that the CSP has validated within its own operations
- The service option that the client has selected to engage the CSP (IaaS, PaaS or SaaS)
- The scope of any additional services the CSP is providing to proactively manage the client’s compliance (for example, additional managed security services)
PCI SSC Guidance

Define Responsibilities such as in the following example:

### Cloud Layer
- Data
- Interfaces (APIs, GUIs)
- Applications
- Solution Stack (Programming languages)
- Operating Systems (OS)
- Virtual Machines
- Virtual network infrastructure
- Hypervisors
- Processing and Memory
- Data Storage (hard drives, removable disks, backups, etc.)
- Network (interfaces and devices, communications infrastructure)
- Physical facilities / data centers

<table>
<thead>
<tr>
<th>Cloud Layer</th>
<th>Service Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Interfaces (APIs, GUIs)</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td>Solution Stack (Programming languages)</td>
<td></td>
</tr>
<tr>
<td>Operating Systems (OS)</td>
<td></td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>Virtual network infrastructure</td>
<td></td>
</tr>
<tr>
<td>Hypervisors</td>
<td></td>
</tr>
<tr>
<td>Processing and Memory</td>
<td></td>
</tr>
<tr>
<td>Data Storage (hard drives, removable disks, backups, etc.)</td>
<td></td>
</tr>
<tr>
<td>Network (interfaces and devices, communications infrastructure)</td>
<td></td>
</tr>
<tr>
<td>Physical facilities / data centers</td>
<td></td>
</tr>
</tbody>
</table>
PCI SSC Guidance

Define Responsibilities such as in the following example:

<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>Example responsibility assignment for management of controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Install and maintain a firewall configuration to protect cardholder data</td>
<td>IaaS</td>
</tr>
<tr>
<td>2: Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>Both</td>
</tr>
<tr>
<td>3: Protect stored cardholder data</td>
<td>Both</td>
</tr>
<tr>
<td>4: Encrypt transmission of cardholder data across open, public networks</td>
<td>Client</td>
</tr>
<tr>
<td>5: Use and regularly update anti-virus software or programs</td>
<td>Client</td>
</tr>
<tr>
<td>6: Develop and maintain secure systems and applications</td>
<td>Both</td>
</tr>
<tr>
<td>7: Restrict access to cardholder data by business need to know</td>
<td>Both</td>
</tr>
<tr>
<td>8: Assign a unique ID to each person with computer access</td>
<td>Both</td>
</tr>
<tr>
<td>9: Restrict physical access to cardholder data</td>
<td>CSP</td>
</tr>
<tr>
<td>10: Track and monitor all access to network resources and cardholder data</td>
<td>Both</td>
</tr>
<tr>
<td>11: Regularly test security systems and processes</td>
<td>Both</td>
</tr>
<tr>
<td>12: Maintain a policy that addresses information security for all personnel</td>
<td>Both</td>
</tr>
<tr>
<td>PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</td>
<td>CSP</td>
</tr>
</tbody>
</table>

PCI SSC Guidance: Segmentation

• Segmentation on a cloud-computing infrastructure must provide an equivalent level of isolation as that achievable through physical network separation.

• Other client environments running on the same infrastructure are to be considered untrusted networks.

• The CSP needs to take ownership of the segmentation between clients.

• The client is responsible for the proper configuration of any segmentation controls implemented within their own environment.
PCI SSC Guidance: Recommendations for Reducing Scope

• Don’t store, process or transmit payment card data in the cloud

• Implement a dedicated physical infrastructure that is used only for the in-scope cloud environment

• Minimize reliance on third-party CSPs for protecting payment card data
PCI SSC Guidance: Compliance Challenges

- Clients may have little or no visibility into the CSP’s underlying infrastructure and the related security controls.
- Clients may have limited or no oversight or control over cardholder data storage.
- Some virtual components do not have the same level of access control, logging, and monitoring as their physical counterparts.
- Perimeter boundaries between client environments can be fluid.
- Public cloud environments are usually designed to allow access from anywhere on the Internet.
• It can be challenging to verify who has access to cardholder data processed, transmitted, or stored in the cloud environment.

• It can be challenging to collect, correlate, and/or archive all of the logs necessary to meet applicable PCI DSS requirements.

• Organizations using data-discovery tools to identify cardholder data in their environments, and to ensure that such data is not stored in unexpected places, may find that running such tools in a cloud environment can be difficult and result in incomplete results.

• **Many large providers might not support right-to-audit for their clients.** Clients should discuss their needs with the provider to determine how the CSP can provide assurance that required controls are in place.
Is AWS 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. Achieving PCI DSS 2.0 validation for AWS helps our customers obtain their own PCI certification.

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. Moving the cardholder environment to AWS can simplify your own PCI compliance by relying on our PCI Compliance. If your QSA currently needs additional supporting information, please contact us at awscompliance@amazon.com.
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.
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.
Sample Cloud Provider Stances: RackSpace

Private clouds are ideal when you need to accelerate innovation, have large compute and storage requirements, or have very strict control, security, and compliance needs.
PCI SSC Guidance: CSP Compliance Notes

- Use of a PCI DSS compliant CSP does not result in PCI DSS compliance for the clients
- An Attestation of Compliance (AOC) reflects a single point in time only
- CSP compliance does not automatically transfer to the client environments within that cloud service
- A client’s PCI DSS compliance does not result in any claim of compliance for the CSP
CSPs should provide their clients with evidence that clearly identifies:

- What was included in the scope of their PCI DSS assessment
- Specific PCI DSS requirements that the environment was assessed against
- Date of the assessment

All aspects of the cloud service *not* covered by the CSP’s PCI DSS assessment should be identified and documented.
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
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?
Considerations
(Continued)

• 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.