Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL RELEASES PCI DSS CLOUD COMPUTING GUIDELINES

— PCI Special Interest Group offers guidance for securing payment card data in cloud environments —

WAKEFIELD, Mass., February 07, 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards published the *PCI DSS Cloud Computing Guidelines Information Supplement*, a product of the Cloud Special Interest Group (SIG). Businesses deploying cloud technology can use this resource as a guide for choosing solutions and third-party cloud providers that will help them secure their customer payment data and support PCI DSS compliance.

PCI Special Interest Groups (SIGs) are community-driven initiatives that provide additional guidance and clarifications or improvements to the PCI Standards and supporting programs.

PCI Participating Organizations selected cloud computing as a key area to address via the SIG process. More than 100 global organizations representing banks, merchants, security assessors and technology vendors collaborated on this guidance designed to help companies identify and address the security challenges for different cloud architectures and models, and understand their PCI DSS responsibilities when implementing these solutions.

“One of cloud computing’s biggest strengths is its shared-responsibility model. However, this shared model can magnify the difficulties of architecting a secure computing environment,” said Chris Brenton, a PCI Cloud SIG contributor and director of security for CloudPassage. “One of this supplement’s greatest achievements is that it clearly defines the security responsibilities of the cloud provider and the cloud customer. With PCI DSS as the foundation, this guidance provides an excellent roadmap to crafting a secure posture in both private and public cloud.”
The *PCI DSS Cloud Computing Guidelines Information Supplement* builds on the work of the 2011 Virtualization SIG, while leveraging other industry standards to provide guidance around the following primary areas and objectives:

- **Cloud Overview** – provides explanation of common deployment and service models for cloud environments, including how implementations may vary within the different types.

- **Cloud Provider/Cloud Customer Relationships**– outlines different roles and responsibilities across the different cloud models and guidance on how to determine and document these responsibilities.

- **PCI DSS Considerations** – provides guidance and examples to help determine responsibilities for individual PCI DSS requirements, and includes segmentation and scoping considerations.

- **PCI DSS Compliance Challenges**- describes some of the challenges associated with validating PCI DSS compliance in a cloud environment.

- **Additional Security Considerations** – explores a number of business and technical security considerations for the use of cloud technologies.

The document also includes a number of appendices to address specific PCI DSS requirements and implementation scenarios, including: additional considerations to help determine PCI DSS responsibilities across different cloud service models; sample system inventory for cloud computing environments; sample matrix for documenting how PCI DSS responsibilities are assigned between cloud provider and client; and a starting set of questions that can help in determining how PCI DSS requirements can be met in a particular cloud environment.

The information supplement can be downloaded from the documents library on the PCI SSC website at https://www.pcisecuritystandards.org/security_standards/documents.php.

Merchants who use or are considering use of cloud technologies in their cardholder data environment and any third-party service providers that provide cloud services or cloud products for merchants can benefit from this guidance. This document may also be of value for assessors reviewing cloud environments as part of a PCI DSS assessment.

As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

"At the Council, we always talk about payment security as a shared responsibility. And cloud is by nature shared, which means that it's increasingly important for all parties involved to understand their responsibility when it comes to protecting this data," said Bob Russo, general manager, PCI Security Standards Council. "It's great to see this guidance come to fruition, and we're excited to get it into the hands of merchants and other organizations looking to take advantage of cloud technology in a secure manner."

Those interested in learning more about this guidance and how to use it are invited to join the PCI Council for a webinar on **February 7 and 14, 2013**. Visit the PCI SSC website for more information and to register: https://www.pcisecuritystandards.org/training/webinars.php.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council

Join the conversation on Twitter: http://twitter.com/#!/PCISSC