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 RISK ASSESSMENT GUIDELINES

— PCI Special Interest Group offers guidance for identifying, analyzing and documenting risks to cardholder data —

WAKEFIELD, Mass., November 16, 2012 —The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today released the *PCI DSS Risk Assessment Guidelines Information Supplement*, a product of the PCI Risk Assessment Special Interest Group (SIG). Organizations planning and performing a risk assessment in accordance with PCI DSS 12.1.2 can use the information supplement to help identify threats and the associated vulnerabilities that could jeopardize the security of payment card data.

PCI Special Interest Groups (SIGs) are Council-led groups made up of industry stakeholders that focus on addressing the need for additional guidance and clarifications or improvements to the PCI Standards and supporting programs. PCI DSS Requirement 12.1.2 requires organizations to establish a formal process for identifying threats and vulnerabilities that could negatively impact the security of cardholder data. By performing this risk assessment, businesses are better equipped to determine the appropriate controls for reducing the likelihood and/or the impact of potential threats to their business.

“As there are a number of risk assessment methodologies out there, our stakeholders were looking for guidance on how to effectively apply these principles to their organizations to meet PCI requirements,” said Bob Russo, general manager, PCI Security Standards Council. “Through our community-driven SIG election process, our Participating Organizations selected this as a key focus area, and the result is a strong set of best practices to guide you through choosing the risk management approach that works best for your business.”

More than 60 organizations representing banks, merchants, security assessors and technology vendors collaborated to produce this guidance that will help organizations understand how to identify, analyze and document the risks that may affect their Cardholder Data Environment (CDE); prioritize risk-mitigation efforts to address the most critical risks first and more effectively implement threat-reducing controls; and determine how to effectively segment environments to isolate sensitive networks (such as the CDE) from non-sensitive networks, as part of an effective scoping methodology.

The information supplement outlines the relationship between PCI DSS and risk assessments; the various industry-recognized risk methodologies and key components of a risk assessment, including developing a risk assessment team and building a risk assessment methodology; risks introduced by third parties; as well as the risk reporting process and critical success factors.

Key recommendations include:

- Organizations should implement a formalized risk assessment methodology that best suits the culture and requirements of the organization
- A continuous risk assessment process enables ongoing discovery of emerging threats and vulnerabilities, allowing an organization to mitigate such threats and vulnerabilities in a proactive and timely manner
- Risk assessments must not be used as a means of avoiding or bypassing applicable PCI DSS requirements (or related compensating controls)

Any organization that stores, processes, or transmits cardholder data can benefit from this guidance, including merchants, service providers, acquirers (merchant banks) and issuers. 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.

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

“As an open standards body, SIGs are one of the many ways we’re able to tap into the brain trust that is our global community. We’re appreciative to all those involved in the Risk Assessment SIG and thank them for their valuable contributions to payment card security through this useful resource,” added Russo.

The guidance on risk assessment is the first of three current SIG projects. Guidance on ecommerce security and cloud computing will be published in early 2013. Additionally, earlier this month Participating Organizations took part in an election to choose SIG projects for 2013. Results will be shared at the end of November, with SIGs to formally commence in January 2013. For the latest updates on SIGs, please visit https://www.pcisecuritystandards.org/get_involved/special_interest_groups.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

###