Why PCI DSS 3.0?

To stay competitive in terms of security and compliance, organizations need a structured, predictable, and continuous approach to solving ongoing challenges that's easy enough to do every day. By raising security standards and making PCI DSS compliance the status quo, organizations can monitor the effectiveness of their security controls and maintain their PCI DSS compliant environment.

PCI DSS 3.0 helps organizations focus on security, not compliance, by making payment security business-as-usual. How?

**1. Increased Education and Awareness**

- Organizations can implement the password strength that is appropriate for their security strategy.
- Greater flexibility recognizes there is more than one way to do security, allowing organizations to choose the approach that works best for their business.

**What's New?**

- **Req. 8.2.3** - Allows for organizations to implement the password strength that is appropriate for its security strategy
- **Req. 15.6** - More flexibility to prioritize log reviews based on an organization’s risk management strategy

For more on what’s new, go to PCI SSC.org

**2. Greater Flexibility**

- 63 percent of investigations identifying a security deficiency easily exploited by hackers revealed a third party responsible for system support, development, or maintenance.
- Many businesses are adopting an outsourced, third-party IT operations model, but this can be a security risk.
- As industry leaders, we need to work together to manage risks and keep information secure.

**What's New?**

- **Guidance on outsourcing PCI DSS responsibilities**
- **Req. 12.8** – PCI DSS responsibilities for service providers

For more on what’s new, go to PCI SSC.org

**3. Security as a Shared Responsibility**

- By increasing awareness and education across organizations, we can help drive payment security as good business practice.

**What's New?**

- Best practices for implementing security into business-as-usual activities to maintain on-going PCI DSS compliance
- Navigating the PCI DSS guidance added for easier understanding of each requirement and security goal
- **Req. 8.4** – Password education for users
- **Req. 9.9** – POS security training and education

For more on what’s new, go to PCI SSC.org

PCI DSS 3.0 helps organizations focus on security, not compliance, by making payment security business-as-usual. How?

**Security DON’Ts**

- Be careless with clients’ payment methods/data
- Fall for phishing scams
- Use weak passwords

Potential Payment Processing Failure Points

- In-house Single Point
- Outsourced Multiple Points

Following PCI DSS is not only good for business, 9 out of 10 security professionals recommend it for payment security.

**Sources**

- Maintaining PCI Compliance: Assess the Impact of Changes in Business, Technology, and PCI DSS, Anton Chuvakin, Gartner Research
- Verizon 2011 Payment Card Industry Compliance Report
- Trustwave 2013 Global Security Report
- Verizon 2013 Data Breach Investigation Report
- Trustwave 2013 Global Security Report
- Real Cost of Security Report (group size: 451)

**PCl Security Standards Council**

For more information on how to make sure your company is aware of its PCI DSS responsibilities, go to PCI SSC.org