Payment Card Industry Data Security Standard (PCI DSS) 3.2

WHAT IS PCI DSS 3.2?

PCI DSS 3.2 is the latest version of the data security standard for payment data.

The new version, published in April 2016, replaces version 3.1 (with immediate effect for all new assessments) and aims to address growing threats to customer payment information. The update to the standard is part of the regular process for ensuring that PCI DSS addresses current challenges and threats.

PCI DSS 3.1 will be retired on October 2016 and from then on all assessments will need to use version 3.2. Whilst some of the amendments to controls will be mandatory from day one, the majority of the requirements introduced will be considered best practice until 31st January 2018. From 1st February 2018 they are effective as requirements.

WHO IS AFFECTED?

All organisations that store, process or transmit payment card data or can impact the security of payment card data must comply with PCI DSS although different levels of compliance apply depending on the number of transactions handled.

This includes:

- merchants;
- resellers;
- card processing bureaux;
- data storage entities;
- web hosting and software application providers;
- acquirers;
- shopping cart and payment service providers; and
- third party agents and vendors of software.

CONSEQUENCES OF NON-COMPLIANCE

If an organisation suffers a data breach and customer information is compromised, lack of PCI DSS compliance could see fines levied by card scheme operators for loss of data.

Organisations may also be liable for financial losses incurred against cards and the operational costs associated with replacing the accounts.

Reputational damage is also a major consideration and a serious data breach could lead to loss of confidence among customers, investors, funders and suppliers.

WHAT IS CHANGING?

The key changes in version 3.2 are aimed at ensuring that critical data security controls remain in place throughout the year and that they are effectively tested as part of the ongoing security monitoring process. PCI DSS 3.2 emphasises a focus within organisations on people, processes and policies with technology playing an important role in reducing the overall cardholder data footprint.

The PCI Security Standards Council stated that since the release of the previous version of the standard there had been an increase in attacks that circumvent a single point of failure, allowing criminals to access systems undetected and to compromise card data.

A significant change in PCI DSS 3.2 aimed at addressing this is including multi-factor authentication as a requirement for any personnel with administrative access to environments handling card data. Previously this requirement applied only to remote access from untrusted networks.

Multi-factor authentication means that at least two or more credentials – such as a password and a smart card - must be used to authorise access to card data and systems. A password alone is not enough to verify a user's identity, even if they are within a trusted network.

Organisations will need to review how they manage authentication for cardholder data environments in light of the changes.

The changes in PCI DSS 3.2 emphasise the importance of validating that security controls are in place and working at all times as part of a business as usual process.

There is a new requirement for service providers to perform penetration testing on segmentation controls at least every six months and to perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.

Responsibilities for the protection of cardholder data and a PCI DSS compliance programme also have to be established by executive management of service providers.

GEMSERV AND PCI DSS

Gemserv's background in Information Security Management Systems enables us to take a unique approach to help ensure cost-effective compliance to PCI DSS.

There is also a shift across the PCI community for compliance to move away from annual assessment activity towards an ongoing risk reduction framework, an area in which Gemserv has significant expertise.

Our approach addresses the wider operational culture, people and processes as much as technology. Risk around PCI DSS is assessed against organisational objectives, reviewing processes before and as appropriate controls are considered.

Gemserv's PCI-DSS services include:

- compliance gap analysis;
- policy development;
- implementation and technical review;
- remediation;
- culture change and transformation;
- assessments;
- SAQ completion / AoC / RoC; and
- training & awareness.

CONTACT US

To find out more about PCI DSS, please contact one of our team on:

E: bd@gemserv.com
T: +44 (0)207 090 1091
W: www.gemserv.com
@gemservinfosec

London Office

8 Fenchurch Place
London
EC3M 4AJ

Ireland Office

Fitzwilliam Hall Business Centre
Fitzwilliam Place
Dublin 2

Company Reg. No: 4419878