PCI DSS – the common questions

We only take a small amount of credit card payments – do we still need to comply?

Yes, PCI DSS compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.

PCI DSS appears difficult – where do I start?

First download and read the PCI DSS standard and familiarise yourself with it. Whilst understanding and implementing the 12 requirements of PCI DSS can seem daunting, it mostly calls for good, basic security. So become familiar with the best practices for security contained in the standard – these are steps that every business should want to take to protect sensitive data and continuity of operations.

Why would I get compliance through a qualified assessor (QSA) like BSI?

An on-site security assessment is a requirement for large merchants with complex IT environments. Whilst other options are available for smaller merchants, such as pre-agreed internal assessments or self-assessment questionnaires, they don't offer the same impartiality or credibility as using an external assessor to review your system. Plus you go beyond checking your compliance at one moment in time, and commit to continual assessment, ensuring your payment card security is maintained over time.

Does PCI DSS make organizations store cardholder data?

Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card, or equivalent data from a chip. If merchants or processors have a business reason to store front-of-card information, such as cardholder name and primary account number (PAN), PCI DSS requires this data to be protected, and the PAN to be encrypted or otherwise made unreadable.

What does PCI DSS mean if we outsource card processing?

You still have responsibilities such as addressing policies and procedures for cardholder transactions and data processing. You need to protect cardholder data when you receive it, and when you process charge backs and refunds. You're also responsible for ensuring that outsourced providers' have applications and card payment terminals that comply with the relevant PCI standards and that they do not store sensitive cardholder data.

Is PCI DSS compliance an IT project?

Absolutely not. PCI compliance is a business issue. The risks of compromise are financial and reputational, so they affect the whole organization. The IT staff will be involved to help implement technical and operational system requirements but compliance requires the business to commit to ongoing assessment, and reporting.

bsi.

Find out more
Call: +44 (0)345 080 9000
Visit: bsigroup.com