PCI Consulting Australia

Compliance with the Payment Card Industry Data Security Standard (PCI DSS)

COMPLIANCE BENEFITS

- Increased security levels
- Avoid loss of reputation and public trust in case of breach
- Avoid Card Scheme penalties for non-compliance
- Full protection from penalties if breached when compliant
- Enhanced information security reputation
- Extra customer comfort level
- Sales opportunity to vend 'compliant services'

NON-COMPLIANCE RISKS

- Increased risk of data breach
- Significant damage to reputation and public trust when systems are breached, taking off your bottom line
- Potential for non-compliance fines
- Substantial fines imposed for any data breach
- Potential loss of right to conduct business using credit/debit card for payments

WHAT IS A QSA?

Qualified Security Assessors (QSAs) are industry experts on hand to assist businesses reach PCI compliance. They complete ROC assessments and assist in SAQ assessments. They have to meet strict criteria set by the PCI SSC which involves security, confidentiality and specific knowledge requirements to be accredited.

PCI Consulting Australia is a hands-on firm operating exclusively within the PCI DSS. It has a proven track record in designing tailored solutions to clients based on their environment and capabilities.

PCI DSS Explained

If your business accepts card payments, you must comply with the PCI DSS. The Payment Card Industry Data Security Standard (PCI DSS) is a global standard designed to protect sensitive card data including account numbers, expiry dates, names and security codes.

To be PCI Compliant, businesses need to either complete a Self Assessment Questionnaire (SAQ) or undertake a detailed assessment in the form of a Report on Compliance (ROC) on an annual basis. The nature of the assessment depends on your merchant level, determined by your "Acquiring" Bank. The greater your transaction volume, the greater likelihood a ROC is required.

Being PCI compliance does not guarantee against a data breach but it does validate that you are taking all appropriate measures to avoid an incident.

PCI SSC

The PCI Security Standards Council is comprised of Visa, MasterCard, JCB, Discover and Amex and sets the global rules for PCI compliance. It provides all the official requirements for compliance as well as numerous reference guides. There is a range of differing SAQs available dependent on how you take card payments, with a reduction in PCI scope where compliant third parties such as payment gateways are used. More information can be found at www.pcisecuritystandards.org

PCI Compliance Best Practice

- Ensure all relevant business units buy into PCI Compliance. This includes IT, HR, Procurement, Finance, Operations and Facilities
- Get your scope right. Have you included all areas of the business that take card payments or have the ability to affect the security of card data? Think call recording systems, email, Windows Updates and web hosts as a few examples
- Undertake a gap analysis which assesses current security against the PCI DSS. It is strongly recommended to use a Qualified Security Assessor (QSA) for this task
- Develop a complete plan to remediate all items which considers budget, operational, resource, and compliance requirements
- Undertake a vulnerability scan on external facing IP addresses. This must be completed by an Approved Scanning Vendor (ASV). https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
- Remediate all items then re-assess to validate
- Develop controls to maintain compliance. An assessment is only at a point in time and accountability for maintaining compliance is up to each business

PCI CONSULTING AUSTRALIA SERVICES AVAILABLE

Advisory Services
Assisted SAQ Assessments
Full ROC Assessments
Acquiring Bank liaison
100% vendor independence
Penetration Testing

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

1300 997 290
www.pciconsultingaustralia.com.au
info@pciconsultingaustralia.com.au