ONE COMPLIANCE

ADVISORY - AUDIT - COMPLIANCE

ABOUT US

We are a data privacy and cyber security specialist who concentrate on increasing the robustness of our clients' security posture using a pragmatic approach.

Our team of well qualified consultants and QSAs can assist with reducing the complexity of security, risk, and compliance projects.

Contact us

To enquire about any of our services:

sales@onecompliance.co.uk

44 (0)20 3290 6547

One Compliance Cyber Limited

Reg Office:
No1 Leeds, 26 Whitehall Road,
Leeds, LS12 1BE

Company No: 08890330

PENTRATION TESTING

A penetration tester will actively attempt to exploit weaknesses in order to gain access to your critical systems.

CISO

A Chief Information Security Officer (CISO) directs staff across the enterprise to reduce information and technological risks.

PCI DSS

One Compliance Qualified Security Assessors (QSAs) take an approach to PCI DSS which reduces both the risk to cardholder data and the ongoing cost of maintaining PCI DSS compliance.

VULNERABILITY ASSESSMENT

A Vulnerability Assessment provides a reasonable level of assurance that the system components which are operated by your business are secured.

DPOaaS

As your Data Protection Officer as a Service (DPOaaS) provider, One Compliance would assume the role of Data Protection Officer in line with Data Protection regulations

ISO27001:2013

ISO 27001 specifies an Information Security Management System (ISMS) that is intended to formalise the management of information security.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that directly handle or impact the security of payment card data.

The PCI DSS was created to reduce payment card fraud. It is an information security standard which is mandated by the five leading global payment card brands and administered by the Payment Card Industry Security Standards Council.

Compliance Levels and Validation

All organisations requiring PCI DSS compliance must assess annually, with specific documentation generated in order to prove PCI DSS compliance.

For VISA and MasterCard, there are four levels of PCI DSS compliance and these are generally based on how many payment card transactions are processed per year:

- Level 1 – Over 6,000,000 transactions annually
- Level 2 – Between 1,000,000 and 6,000,000 transactions annually
- Level 3 – Between 20,000 and 1,000,000 transactions annually
- Level 4 – Less than 20,000 transactions annually

Other card brands (American Express, Discover, JCB) operate different compliance levels and transaction volumes.

Level 1 merchants must validate PCI DSS compliance using a PCI DSS Qualified Security Assessor (QSA).

Level 2 MasterCard merchants must validate PCI DSS compliance using a PCI DSS Qualified Security Assessor (QSA).

Level 2 VISA merchants can self-assess through the Self-Assessment Questionnaire.

Level 3 and 4 merchants can self-assess through the Self-Assessment Questionnaire.

The output of a formal QSA-led PCI DSS assessment is a Report on Compliance (RoC) and Attestation of Compliance (AoC).

Self-assessments can also be validated by a QSA to ensure that the compliance had been properly validated.

HOW CAN ONE COMPLIANCE HELP?

One Compliance are a PCI DSS Qualified Security Assessor Company (QSAC). A Qualified Security Assessor (QSA) is an individual certified by the PCI Security Standards Council to conduct PCI DSS assessments, and produce the RoC and AoC documentation to validate PCI DSS compliance.

The secret to maintaining compliance for PCI DSS is not to meet the standard, but to avoid the standard. This process is known as Descoping.

Descoping begins with an evaluation of your business processes in order to identify opportunities to reduce the impact of PCI DSS. This examines each payment channel with a view to reduce the number of PCI DSS controls which are applicable, and what technical options are available to isolate each business process which has a PCI DSS impact.

One Compliance specialise in reviewing the PCI DSS landscape by carefully understanding the business processes within each of your payment channels:

- What is the maximum scope reduction which can be achieved?
- What level of scope reduction is acceptable to the organisation?
- How much effort is likely to be required to change business processes on order to reduce PCI DSS scope?
- What opportunities are available to outsource payment card processes and who are appropriate partners?

Descoping reduces the ongoing cost of PCI DSS compliance and reduces the risk of payment card processing. The PCI DSS standard evolves on a 3-year cycle. New controls are introduced, guidance is updated, maintaining compliance becomes more difficult. The benefits of descoping become greater as PCI DSS evolves as an information security standard.

Whether you need a descoping options analysis, a gap analysis, a pre-assessment of controls, an assessment to complete a RoC and AoC, or assistance with your Self-Assessment Questionnaire (SAQ) it's always worth engaging a QSA to ensure that you are mitigating your risk against potential breach and subsequent fines, penalties and PR headaches.

Further details can be found at

www.onecompliance.co.uk or by contacting:
sales@onecompliance.co.uk