PCI DSS - Demystify and Comply

Simplifying and Demystifying Compliance with the current Payment Card Industry Data Security Standard (PCI DSS)

February 2024 - v1.2

If you accept or process debit and credit payment cards, PCI DSS applies to you.

The **PCI Data Security Standard (PCI DSS) applies to all entities that store, process, and/or transmit cardholder data**. It covers technical and operational practices for system components included in or connected to environments with cardholder data.

PCI DSS follows common-sense steps that mirror security best practices. PCI DSS applies globally to all entities that store, process or transmit cardholder data and/or sensitive authentication data. PCI DSS and related security standards are administered by the **PCI Security Standards Council (SSC)**, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Participating Organizations include merchants, payment card issuing banks, processors, developers and other vendors.

The PCI DSS

PCI DSS specifies 12 requirements entailing many security technologies and business processes and reflects most of the usual best practices for securing sensitive information; the resulting **scope is comprehensive and may seem daunting**.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

There are many myths commonly associated with implementing and maintaining compliance with the latest PCI DSS; **UKDataSecure has over 15 years' experience working with multiple level 1 UK and global merchants**, demystifying PCI DSS requirements and simplifying compliance.

Every entity accepting or processing debit and credit payment cards, regardless of size and volume of payment card transactions accepted, is required by their acquiring bank to achieve and maintain PCI DSS compliance; whilst the scope is comprehensive it shouldn't be overly complex.

PCI DSS mostly calls for good, basic security measures and the best practices for security contained in the standard are steps that every business should want to take anyway to protect sensitive data and continuity of operations.

UKDataSecure always strongly recommends that **achieving and maintaining PCI DSS compliance should be part and parcel of any organisations ongoing data, information and cyber security program**.

Many of the data security measures organisations will be implementing to meet other regulatory, legislative and security control framework requirements, such as the UK Data Protection Act 2018 incorporating GDPR, ISO27001, NIST and Cyber Essentials will apply equally to PCI DSS.

PCI DSS COMPLIANCE

UKDataSecure Ltd | https://www.ukdatasecure.com | 02380 972066 | 07824 445375 | info@ukdatasecure.com
Registered Office: Bencroft, Dassels, Braughing, Ware, Hertfordshire, SG11 2RW | Registered in England and Wales, Registration No: 6885551

UKDataSecure's approach to demystifying and simplifying clients' PCI DSS journey **always starts with a simple PCI Compliance Assessment**, with the fundamental objective of being able to **determine how 'PCI attestation of compliance ready' a business is in each payment channel.**

Such a compliance assessment typically consists of a minimum two day 'on-site' discovery and gap analysis exercise.

Discovery and Gap Analysis

During the discovery and gap analysis we will attend client locations and spend time in conversation with multiple key business and information technology stakeholders, and will observe and define:

- Payment card channels and transaction volumes
- Methods by which payments are taken by card
- Associated systems interfaces
- PCI controls applicable by payment channel
- Current demands and timescales from acquirers
- Current high-level PCI compliance status estimate
- Priorities and opportunities for scope reduction
- Proposed outline roadmap to achieve compliance

Prioritisation and Descoping Opportunities

Key to UKDataSecure's 'demystify and simplify' approach is to work with clients to prioritise what must be fixed first, where budgets should be spent first and how specific parts of payment channels can be descoped and therefore PCI compliance be simplified.

PCI DSS COMPLIANCE

We document the outputs of our discovery and gap analysis compliance assessment exercise and present back the findings to clients in person, suggesting high level recommendations and options possible for clients to achieve PCI compliance, in a sustainable way that will allow clients to maintain PCI compliance and achieve re-attestation in subsequent years.

UKDataSecure will then subsequently work with clients to develop detailed strategies, plans and next steps, to achieve PCI compliance by individual payment channel, and can assist clients with all aspects of achieving and maintaining PCI compliance.

Our key PCI compliance competencies include:

- PCI Program Management and Governance
- Card-Holder Data Risk Assessment
- Policy Procedure and Process Review and Writing
- Incident Response Planning
- Security Training and Awareness
- Third Party Service Provider Validation

UKDataSecure constantly references and uses resources published by the PCI SSC on their website, along with the PCI DSS itself; please follow this link to get started with the extensive library of PCI SSC resources available:

https://www.pcisecuritystandards.org/merchants/

I look forward to talking through the details of our Demystify and Comply services with you as soon as we can, and I look forward to working with you to achieve PCI DSS compliance as part of an holistic data risk management and information security governance and compliance program.

Stuart Golding - Founder and CEO

UKDataSecure Ltd | https://www.ukdatasecure.com | 02380 972066 | 07824 445375 | info@ukdatasecure.com
Registered Office: Bencroft, Dassels, Braughing, Ware, Hertfordshire, SG11 2RW | Registered in England and Wales, Registration No: 6885551