GALA TECHNOLOGY

SOTpay®

WHAT IS PCI-DSS COMPLIANCE?

A Concise Guide

Everything you need to know about PCI-DSS and why its a fundamental role in your business

Decoding PCI Compliance: What It Is and Why It Matters

PCI DSS, or the Payment Card Industry Data Security Standard, is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. This standard is essential for protecting cardholder data and reducing the risk of data breaches in the payment card industry. It applies globally to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers.

It's crucial for your organisation to protect customers' payment data, including sensitive card numbers and Sensitive Authentication Data (SAD), from both internal and external fraudulent attacks and security breaches. Achieving PCI compliance ensures the safe processing of such data.

Additionally, the General Data Protection Regulation (GDPR) imposes strict rules on handling personal information. Non-compliance can lead to substantial fines from the Information Commissioners Office (ICO). Hence, adopting best practices in data security across all corporate processes is essential, extending beyond just payment acceptance.

Gala Technology is certified as PCI-DSS Level 1, representing the highest certification level for PCI payments. This demonstrates the commitment to maintaining the most rigorous standards of payment security and data protection.

Evaluating the Impact of PCI-DSS on Your Organisation: A Detailed Analysis

PCI DSS is essential for any organisation that handles card data, as it safeguards against the constant threat of data theft by hackers. This standard is crucial regardless of business size, as it protects customer data and helps prevent data breaches, which can have significant impacts. PCI DSS serves as a protective measure for both customers and the business itself.

Identifying the Enforcers of PCI Compliance: Understanding Their Role and Authority

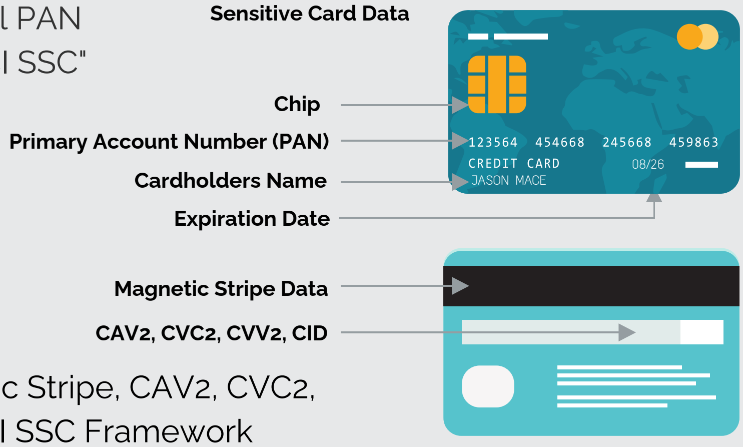
The Genesis and Evolution of the PCI Security Standard: Initiated by Visa, Mastercard, American Express, Discover, and JCB on December 15, 2004, and the Formation of the PCI Security Standards Council (PCI SSC) in 2006. Understanding the Role of PCI SSC in Administering Guidelines and the Responsibility of Payment Brands and Acquirers in Enforcing Compliance.

Deciphering 'Cardholder Data': Understanding What Constitutes Credit Card Information

The PCI Security Standards Council (SSC) Definition Explained

Exploring 'Cardholder Data': Defining the Full Primary Account Number (PAN) as per PCI SSC. The Full PAN and Its Associated Elements as Specified by PCI SSC"

- Cardholder name
- Expiration date
- Service code



Sensitive Card Data

Chip

Primary Account Number (PAN)

Cardholders Name

Expiration Date

Magnetic Stripe Data

CAV2, CVC2, CVV2, CID

Detailing 'Cardholder Data': Inclusion of Magnetic Stripe, CAV2, CVC2, CVV2, CID, PINs, PIN Blocks, and More in the PCI SSC Framework

Achieving PCI Compliance: Your Essential Guide to Success

To achieve PCI compliance, organisations must adhere to 12 requirements set by the PCI Security Standards Council (SSC). These standards are designed to maximise data protection throughout the payment transaction process, whether conducted manually or electronically. Compliance with these requirements significantly enhances protection against both external and internal security threats. Additionally, the specific reporting obligations an organisation must follow depend on its merchant level, which is determined by the annual volume of transactions processed.

For Merchant Level 1 in PCI compliance, there is a requirement for an on-site assessment to be conducted by a Qualified Security Assessor (QSA). This assessment is a key part of ensuring that the highest level of PCI compliance standards are met and maintained.

For Merchant Levels 2 to 4 in PCI compliance, the process involves self-assessment using Self-Assessment Questionnaires (SAQ). This approach allows these merchants to evaluate and ensure their compliance with PCI standards through a structured self-assessment process.

For PCI compliance, it's mandatory to conduct a quarterly network scan by an Approved Scan Vendor (ASV). Additionally, an attestation of Compliance Form must be completed to demonstrate adherence to the required standards. These steps are vital for ensuring ongoing security and compliance with PCI regulations

Exploring the Different Levels of PCI-DSS Compliance

Organisations are categorised into one of four PCI compliance levels based on their annual transaction volume

- Level 1: Merchants processing over 6 million VISA and Mastercard transactions.
- Level 2: Merchants handling 1 to 6 million VISA and Mastercard transactions.
- Level 3: Merchants with 20,000 to 1 million VISA and Mastercard transactions.
- Level 4: Merchants processing fewer than 20,000 VISA and Mastercard transactions.

A breach involving card payment data can result in an organisation being escalated to a higher compliance level.

Assessing the Risks and Penalties of Non-Compliance with PCI DSS

Understanding PCI DSS: Mandatory for Transaction Processing with Major Card Schemes and the Consequences of Non-Compliance

- Significant fines ranging between £3,000 and £6,000.
- Erosion of customer trust, prompting them to move to other merchants.
- A decline in sales figures.
- Expenses incurred in reissuing new payment cards.
- Financial repercussions stemming from data breaches and fraud incidents.
- Legal implications including costly settlements and judgments.
- Loss of the privilege to process card payments.
- Job losses in key positions such as CISO, CIO, and CEO.
- The potential for the business to shut down.
- Elevated future costs for achieving compliance standards.

If your business isn't PCI compliant and suffers a data breach, your banking provider may impose fines or terminate your ability to process card payments. This can significantly impact your business operations. Compliance is not just a regulatory requirement, but a crucial aspect of maintaining your business's functionality and reputation.

Understanding GDPR Fines: Navigating the Consequences of Non-Compliance

Non-compliance with PCI-DSS leading to a data breach may trigger an investigation by the Information Commissioners Office (ICO) regarding GDPR compliance. This could result in substantial fines, potentially up to €20 million (about £17.5 million) or 4% of annual turnover, whichever is higher, emphasizing the significant financial risks of non-compliance.

Mastering the 12 Key Requirements of PCI DSS: A Comprehensive Overview

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a Security Policy that addresses information security for all personnel.

Each of these requirements is essential for maintaining PCI-DSS compliance.

Learn More

Unveiling the Significance of PCI DSS: Protecting Data and Building Trust

Cardholder Data Security: A Critical Element in the Payment Card Ecosystem. The Impact of Data Breaches on Cardholders and the Broader Payment Process, Highlighting the Necessity of Strong Data Security Measures. Consequences for Customers and Organisations in the Event of Security Failures, Including Loss of Trust and Financial Liabilities.

The Role of Organisations and Financial Institutions in Upholding Security Protocols to Protect Their Operations and Reputation. The Benefits of PCI Compliance in Ensuring Secure Payment Card Transactions, as Advocated by the PCI Security Standards Council (PCI SSC), and Its Contribution to Global Trust in Payment Systems.

Your Path to PCI-DSS Compliance

Achieving PCI compliance independently can be time-consuming, costly, and error-prone. Gala Technology alleviates this burden with established PCI-DSS level 1 compliant payment solutions. They evaluate your systems and offer a secure, tailored platform to suit your organisation's needs.

Navigating PCI DSS and FCA Compliance

FCA regulations require financial firms to record calls for monitoring and training to prevent market abuse. However, PCI-DSS mandates no recording of sensitive card data.

SOTpay addresses both by enabling customers to enter card numbers via phone keypad, allowing full call recording for FCA compliance without logging sensitive data, ensuring PCI compliance.

Demystifying Descoping: Understanding Its Impact and Benefits

In PCI-DSS, anyone or anything interacting with payment data is "in-scope", including call centre agents, telephony systems, and IT networks for payments. Compliance includes meeting 12 PCI-DSS requirements.

To simplify compliance, reduce staff and systems handling card payments by outsourcing to third-party providers like SOTpay, offering PCI compliant payment solutions.

This strategy can expedite and economise PCI compliance, allowing focus on what really matters, your business growth.

Streamline Your PCI Compliance Journey with Gala Technology's Expert Solutions

Gala Technology can assist at any stage of your PCI compliance journey, offering PCI compliant payment services that align with your organisation's operations.

This can significantly reduce PCI risk and requirements, turning a lengthy Self-Assessment Questionnaire from **233 items to just 13 simple yes/no questions**. For guidance on starting your PCI compliance process,

Gala Technology offers consultations on payment processes and compliance strategies.

Trusted by hundreds of clients, handling over £3 billion through various payment services and maintain a constantly updated PCI DSS Level 1 v3.2.1 platform.

ABOUT GALA TECHNOLOGY

Gala Technology offers global, secure cloud payment solutions, enhancing business revenue and customer protection. Their services span across phone payments, automation like secure IVR for 24/7 payments, and communication channels including live web chat, WhatsApp, email, SMS, and social media. Their trusted omni-channel SaaS platform, compliant with PCI-DSS, has onboarded 1200+ merchants and protected £3 billion+ revenue from fraud, serving in 30+ countries. It integrates with leading merchants and payment gateways worldwide, handling over 2.5 million protected transactions.

Secure Your Customers' Trust: Begin Protecting Them Now

Enhance your organisation's security with Gala Technology's PCI-DSS compliant solutions. Tailored to your unique business needs, their services mitigate serious security risks.

Discover more about their payment services, or get in touch at **+44 (0) 1709 911 661** or info@galatechnology.com to discuss specific requirements.

SOTpay™

SECURE . COMPLY. PROTECT.

JASON MACE

CEO - GALA TECHNOLOGY

Start Your Free SOTpay Trial Today! click here

GALA TECHNOLOGY

CONTACT US

+44 (0) 1709 911 661

info@galatechnology.com
www.galatechnology.co.uk