# PCI Launch

The PCI-DSS (Payment Card Industry Data Security Standard) is an industry regulatory standard, written and maintained by the PCI Security Standards Council (PCI SSC), that provides a baseline of technical and operational requirements for organizations that store, process, or transmit cardholder data (CHD) and/ or sensitive authentication data (SAD), or could impact the cardholder data environment (CDE). Components that could be impacted/in scope for PCI-DSS include network devices, servers, computing devices, virtual components, cloud components, and software. PCI-DSS undergoes regular evolution as threats and attacks grow more sophisticated and is currently on version 4.0. HanaByte leads expertise in automating and implementing compliance services and are able to conduct a PCI-DSS readiness assessment tailored to your organization before you initiate a formal PCI-DSS audit. If your bank or other financial institution has not already selected an audit firm, we can provide coaching to select an audit and certification firm appropriate for your business.

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
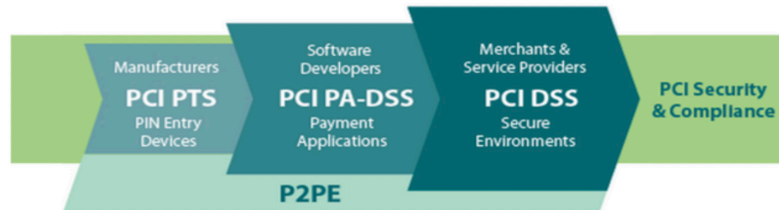
Ecosystem of payment devices, applications, infrastructure and users

Source: https://infoassureltd.com/payment-card-data-security-standard-pci-dss/

Scope

☑ Review of your existing CDE including control implementations, infrastructure, software, people, policies, procedures, and any relevant documentation to perform a gap assessment against the PCI-DSS framework.

☑ Perform workshops about PCI-DSS compliance and procedures - educating key stakeholders, technical personnel, and support teams about compliance and PCI scope. Workshops are interactive and are used to learn more about your business.

Deliverables

☑ Gap assessment report describing HanaByte's findings and recommendations.

☑ Variety of workshops related to PCI compliance/processes.

Personnel

Security Consultant(s), billed 5 days, full-day, per week for the engagement. Resource count based on client business needs.

Customer Responsibilities

Provide access to relevant documentation (including policies, procedures, and diagrams), personnel, in-scope infrastructure and systems.

Our Services

Cloud Strategy & Workshops

Let your best friend in security work with you to develop and execute a robust cloud security strategy. We also offer expert-led interactive workshops to develop security best practices.

Security & Compliance Assessments

Our experts will evaluate your organization's security controls and procedures against industry standards, providing a detailed readiness report and actionable recommendations to achieve your security and compliance goals.

Cloud Migrations & Modernization

We ensure a secure cloud migration/modernization of your applications, data, and infrastructure. Our experts will provide guidance and support throughout the entire process, from planning and execution to post-migration optimization.

DevOps & Security Engineering

Our DevSecOps experts are ready to assist with maturing a software development lifecycle, creating cloud automation, and performing tool integrations to foster secure engineering practices. We specialize in CI/CD, containers, and infrastructure as code.

Application & API Security

Our services provide end-to-end protection for your applications and APIs. Our experts will work with you to implement best practices and the latest technologies to keep your data and systems secure from development to deployment.

Vulnerability Management & Penetration Testing

Our experts use the latest tactics, techniques, and procedures to perform comprehensive security assessments. We go beyond automated tooling to simulate real-world attacks, providing an in-depth analysis of your security posture.

About HanaByte

We are a team of skilled, empathetic individuals with a passion for cybersecurity. We believe in creating a safe and secure online environment for everyone, and we're committed to the pursuit of that goal.

Get In Touch

Hanabyte.com
info@hanabyte.com
404.994.2603

@Hanabyte