



PCI DSS Compliance Program Management Services

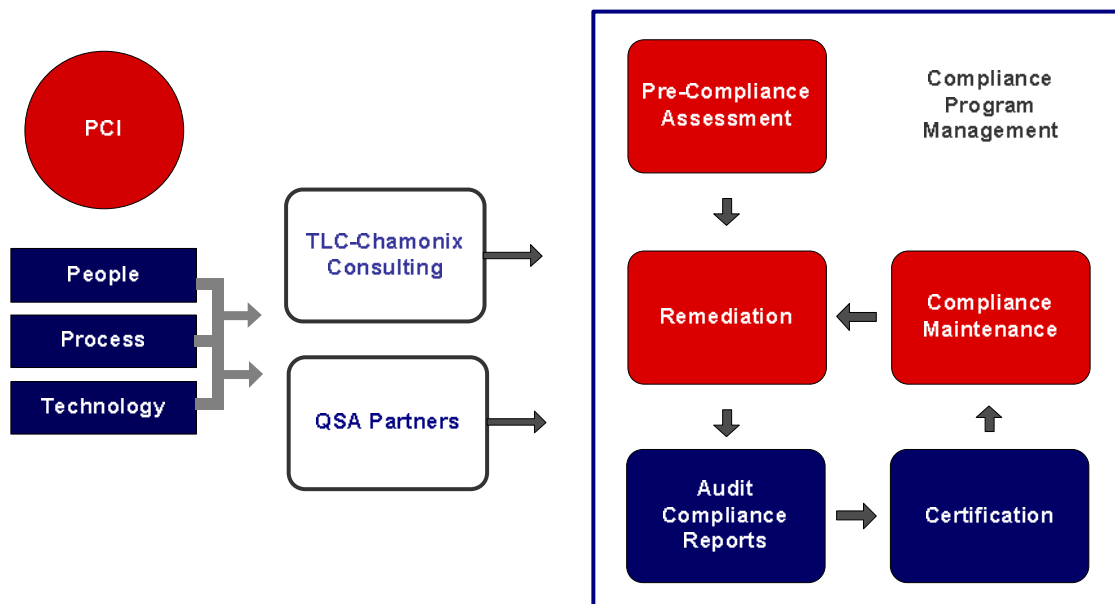
The Payment Card Industry (PCI) Data Security Standard (DSS) is a worldwide standard mandated by Visa, MasterCard, American Express, Discover and JCB International for the protection of cardholder information.

To ensure organizations become compliant with PCI DSS 1.2, TLC-Chamonix, LLC (TLC) has partnered with leading Qualified Security Assessors (QSA) to offer a comprehensive program of compliancy services with a range of options.

TLC and its partners will help your organization to understand the PCI DSS standard and how it fits alongside other security frameworks. This PCI DSS Compliance Program Management Services includes a combination of consulting, analysis tools, network vulnerability scans, program management and status reporting to help guide you through the process of becoming compliant. This approach will help you minimize effort, cost and accelerate certification.

Our PCI DSS compliance program follows security industry best practice and consists of a sophisticated 5-stage approach to achieve and maintain compliance:

1. Pre-compliance Assessment
2. Remediation
3. Compliance Audit Reporting
4. Certification
5. Compliance Maintenance





Stage 1 – Pre-compliance Assessment

The pre-compliance assessment will help you understand the size of the compliance risk to your business and kick-off your compliance program. The pre-compliance assessment is the data gathering process that identifies gaps between your current security position, PCI DSS and other security standards, such as FIPS 140-2.

The pre-compliance assessment will typically include:

- ✚ Conducting on-site review of IT infrastructure, network design, application architecture, policies, procedures and processes to determine non-compliant areas
- ✚ Conducting network vulnerability scanning
- ✚ A gap analysis between the pre-assessment and scan results against both PCI DSS criteria and industry best practice
- ✚ A risk analysis and recommendation report
- ✚ Scoping and prioritizing remediation activities

Stage 2 – Remediation

Based upon the results of the pre-compliance assessment the remediation program provides a controlled, focused and effective framework to achieve compliance. Our remediation program will help your organization develop, implement and document the evidence required to prove compliance.

Policy Development

Our consultants can develop information security policies and practices that incorporate your organization's specific business requirements and IT environment. Our consultant's experience ranges from large multi-channel retailers and financial services organizations to small business networks. The consultant will work with your own staff to develop policies that are targeted at your needs while incorporating the latest security requirements.

Infrastructure Development

Decades of experience in secure network infrastructure design mean that our team can advise your business on how to leverage its infrastructure investment while accommodating PCI DSS requirements, including the effective use of firewalls, intrusion detection and protection and network segmentation.

Security Solutions

TLC, in association with our QSA partners, has extensive experience in deploying a range of security technologies. This includes advanced secure wireless, identity management, key management, penetration detection and audit logging. We can procure and deploy technology-based solutions into your operational environment.



Stage 3 – Compliance Audit Reporting

At the conclusion of the remediation phase TLC and our QSA partner will manage the audit process. This phase will include the production of the Report on Compliance (ROC) for level 1 and a compliance report for level 2 and 3 merchants.

For a level 1 merchant an on-site audit is compulsory and advisable for level 2 merchants. The QSA will assign a consultant to validate compliance (typically by conducting interviews with key staff), perform vulnerability scanning and other defined tests required in the PCI standard. For level 2 and 3 merchants compliance validation can take place remotely through a compliance portal with the QSA consultant ensuring that all areas of the Self Assessment Questionnaire (SAQ) have been covered and remediation tasks identified.

Stage 4 – Certification

This phase is undertaken by the QSA and includes the:

- ✚ Submission of all relevant documentation, including the ROC, to the card schemes for level 1 merchants, and the certification of the audit report by the card schemes
- ✚ For level 2 and level 3 submission of the merchants compliance report to their acquirer

Stage 5 –Compliance Maintenance

Compliance is not a one-time event. PCI DSS certification is required annually and network vulnerability scanning required on either a quarterly or annual basis, depending on your designated compliance level. It is vital that any process or technology decisions are taken with PCI DSS compliance at their heart. Our compliance management service help you avoid potential pitfalls in the decision making process and will ensure that your organization will *remain compliant*.

TLC can manage the overall PCI DSS compliance process, providing program management from the initial pre-compliance assessment through to certification and ongoing compliance. TLC can leverage its relationships with the relevant parties to define key milestones for the project, which would form the basis of the compliance project plan. Compliance planning would typically include:

- ✚ Representing client interests with Visa, MasterCard and the participating banks
- ✚ Providing advice and consultancy on the PCI Data Security Standard and define project scope
- ✚ Providing training and guidance on compliance, monitoring and loss prevention