E COM SECURITY®
SOLUTIONS

Payment Card Industry - Data Security Standards (PCI DSS) Compliance

E Com Security Solutions assist organizations of all sizes achieve compliance with the PCI DSS Standards and also help reduce the risk of breach and strengthen the security posture.

ABOUT PCI DSS STANDARD

The Payment Card Industry Data Security Standard (PCI DSS) was established by the major card brands (MasterCard World wide, Discover Financial Services, American Express, JCB International, and Visa Inc.). All businesses that process, store, or transmit payment card data are required to implement the standard to prevent cardholder data theft.

PCI DSS COMPLIANCE REQUIREMENTS

Compliance levels for merchants and service providers are defined based on annual transaction volume and corresponding risk exposure. All merchants and service providers fall into one of the four levels based upon credit or debit card transaction volume over 12 month period.

GETTING STARTED WITH PCI DSS COMPLIANCE

For small and medium sized businesses (SMBs) — Merchants that transact less than 6 Million payment card transactions in an year are classified as Level 2, Level 3 and Level 4. E Com Security Solutions' help these merchants complete their SAQ, explain identified vulnerabilities, pass the ASV scan, and ensure that their PCI compliance is validated and reported to their merchant processor.

For enterprise organizations — Merchant or service providers that transact more than 6 Million payment card transactions in anyear are classified as Level 1 and must undergo an onsite assessment. E Com Security Solutions' will assign a Qualified Security Assessor (QSA) to validate a company's compliance with the PCI requirements by conducting interviews with business and operations personnel, and perform required tests. Entities found to be compliant will receive a written Report on Compliance (RoC) to be provided to acquiring banks and an Attestation of Compliance (AoC) as a declaration of compliance status.

Fact Sheet

100% of organizations that suffered a breach were not compliant with the PCI DSS standard.

55% of organizations achieved PCI DSS compliance at the interim assessment.

13% is the average percentage of controls were not in place for companies failing their interim assessment.

For more information

Visit www.ecomsecurity.org or E-Mail us at sales@ecomsecurity.org.

PCI COMPLIANCE APPROACH FOR SMALL & MEDIUM BUSINESS

SMBs can demonstrate PCI Compliance by completing the Self-Assessment Questionnaire (SAQ) along with passed ASV scan. However Organizations should also consult their acquirer (merchant bank) or payment brand to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.The required SAQ is dependent on how you store, handle, and process card data. Some additional requirements as below may also include:

- External vulnerability scanning
- Internal vulnerability scanning
- Penetration testing
- Security policy implementation

Determine Your Requirements—We'll access the PCI DSS Scope, Merchant level and based on how you process payment cards your specific PCI questionnaire will be determined.

Pass Your ASV Scan— Businesess that process, store or transmit cardholder data online are required to have external network vulnerability scans performed on their network or domain to identify network vulnerabilities that can impact the card holder data.

Compliance Assessment—Our Consultants will offsite review the current state of compliance against the PCI DSS standards and provide a report to Identify any areas of potential non-compliance, areas that need protection against information security breaches and actionable recommendations. .

Certification—At the end of the engagement your organization is provided with the completed SAQ and the certificate of compliance.

PCI COMPLIANCE APPROACH FOR ENTERPRISE ORGANIZATIONS

E Com Security Solutions' provides services to support organizations' PCI activities throughout all stages – from building a PCI program to performing the assessments required to demonstrate compliance.

Engagement Scoping—Dedicated consultants work closely with organizations to identify and validate all locations, applications and flows of cardholder data to ensure that they are included in the scope of the engagement.

Primary Document Collection & Mapping—The PCI DSS requires documentation and evidence to be collected during the assessment process. We will review and analyze submitted documentation to include all policies, procedures, system configurations, network diagrams, dataflow diagrams and other evidence as required for validating PCI DSS compliance.

On-Site Assessment—We will assign a Qualified Security Assessor (QSA) to validate a company's compliance with the data security requirements by conducting interviews with business and operations personnel, and perform required tests. The QSA will coordinate and schedule activities and resources with the client company and ensure the quality of all the deliverables.

Remediation Support— We provide assistance, consulting and advisory services in the implementation of remediation plans. This may include developing specific implementation plans or consulting on various remediation needs. We also provide Information Security Services to meet other PCI DSS requirements, such as:

- Policy Development
- Development of System Configuration Standards
- Ongoing Identification of New Vulnerabilities
- Web Application Penetration test
- Application Code Reviews
- Vulnerability Scanning & Penetration testing
- Perimeter Security Monitoring (Firewalls, IDS/IPS)
- Log Monitoring/Log Retention
- Third-Party Risk Management
- Security and Risk Consulting

Report on Compliance & Finalization—Entities found to be compliant will receive a written Report on Compliance (RoC) to be provided to acquiring banks and an Attestation of Compliance (AoC) as a declaration of compliance status.

E COM SECURITY® SOLUTIONS

E Com Security Solutions' provide Compliance, Application Security, Infrastructure security and advisory services through the cloud, managed security services and software that help clients protect their most important assets from evolving cyber threats. As the global professional services and consulting network, with approximately 300 security consultants world wide, we bring world-class capabilities and high-quality services to our clients.