PCI DSS
Compliance Services

What is PCI DSS?

PCI DSS, is a mandatory to comply with, standard that specifies the framework for a secure payments environment and presents the common sense steps that mirror best security practices.

Cardholder data is defined as the Primary Account Number ("PAN") and other data, obtained as part of a payment transaction, including the following data elements:

- PAN
- Cardholder Name
- Expiration Date
- Service Code
- Sensitive Authentication Data

Every Organization that stores, transfers or processes the Primary Account Number (PAN) during transactions, must demonstrate compliance with PCI DSS.

Who must comply with PCI DSS?

It is addressed to:

- Acquiring Banks, members of the Card Brand Institutes
- Merchants that accept credit cards in exchange for goods and services
- Third Parties that processes, stores or transmits cardholder data including companies that provide services to merchants or other service providers.

What is PCI DSS Compliance?

PCI DSS is a standard that includes more than 200 security controls for any Organization that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment and present the common sense steps that mirror best security practices.

The goals that must be achieved when complying with PCI DSS requirements are:

1. Building and Maintaining a Secure Network
2. Protecting Cardholder Data
3. Maintaining a Vulnerability Management Program
4. Implementing Strong Access Control Measures
5. Regularly Monitoring and Testing Networks
6. Maintaining an Information Security Policy

How to achieve PCI DSS compliance?

For the total of PCI DSS requirements, ongoing compliance is achieved by the by a continuous 3-step process for continuous improvement "Assess-Remediate-Report".

1. **Assess:** includes the procedures of Risk Assessment, Vulnerability Assessment and Gap Analysis.
2. **Remediate:** includes the process of prioritizing remediation and corrective actions for the identified vulnerabilities and non-conformities based on the results of the risk assessment, vulnerability assessment and gap analysis processes.

beSecure

Managed E-Business Security™

3. **Report:** includes the documentation of deliverables required for proving that the remediation and corrective actions have taken place, that are to be submitted to the relative acquiring bank and/or Card Brands.

Following continuously the above 3 steps, continuous compliance with the requirements of PCI DSS is achieved, but also, an information security framework inside the organization is built.

BESECURE's Methodology approach

BESECURE has developed a methodology appoach that is divided in three major phases:
1. Pre-assessment/Gap Analysis phase
2. Compliance Audit phase
3. Ongoing Compliance phase.

The approach and services that are included in each phase, are shown in the following diagram.

BESECURE's Services and Solutions

BESECURE is activated in the provision of integrated solutions and services in the area of information security and risk management and provides a holistic approach on establishing an information security framework and achieving compliance in an Organization.

For the complete implementation of PCI DSS requirements, BESECURE provides consulting services and solutions from the pre-assessment phase up to certification. More specifically, the services and solutions provided are:

- Risk Assessment & Gap Analysis
- Information Security Policy and Procedures Development Services
- Architecture Design of Systems Information Security Infrastructure
- Design & Development of Information Security Management Systems based on ISO 27001 standard
- Management & Monitoring of the Information Security Infrastructure
- Audit & Security Certification based on international standards and best practices
- Network and Systems Vulnerability Assessments and Penetration Tests
- Information Security Awareness & Training Services
- Firewall and Wireless infrastructure installation and configuration
- Encryption and Data Loss Prevention (DLP) solution provider

About BESECURE

BESECURE, is a leading provider of Governance, Risk & Compliance (GRC) services, Cyber Security solutions, Managed Security services, Certification Training and Awareness programs, ISO 27001 and ISO 9001 certified, trusted by global organizations across telecommunication, financial services, energy industries and other medium - large enterprises to safeguard their information assets including financial information, intellectual property, trade secrets, Personally Identifiable Information (PII) or information entrusted to them by customers or third parties. For more information, please visit http://www.besecuregroup.com.

Greece, Southeast Europe
19, Syngrou Ave., 117 43,
Athens, Greece
Tel. +30 210 330 7 440, Fax +30 210 330 7 441
www.besecuregroup.com

Cyprus, Middle East
133B Fraglin Roosevelt Ave, 3011,
Limassol,Cyprus
Tel. +357 250 29 300, Fax +357 250 29 301

Belgium, Western Europe
Place Rouppe 27,
1000, Brussels, Belgium
Tel. +32 25 88 4470, Fax +32 25 88 4471
info@besecuregroup.com