COMPLIANCE SERVICES

Your Path To Achieving **PCI-DSS Compliance**

Key Benefits Of This Service:

Our bundled compliance solution takes a streamlined approach both on and off-site to get your business ready for its next assessment and keep you compliant all year round. Our expert QSAs know how to effectively implement the processes your organization needs to protect cardholder data and keep sensitive information secure.

Free PCI-DSS Gap Analysis

We compare your cardholder environment's current security controls against the revised requirements and provide an analysis that includes a list of controls that will need to be updated or replaced. This saves time and costs by identifying exactly which services your business needs.

Policies and Procedures Development

Our policy and procedures assistance will alleviate the headaches (and costly mistakes) that many business owners run into while trying to develop these technical documents. Bundling this service with your PCI DSS assessment will save you significant time and money.

Trusted Advisory and Remediation

Included Trusted Advisory and Remediation means that MegaplanIT will assist you with any system changes made throughout the year that might affect your PCI compliance status. This service may actually reduce the time and cost of your PCI assessment year after year!

PCI Compliance Project Management

We monitor your compliance deadlines and tracks milestones completions throughout the year. While two QSAs are conducting your assessment, our management team aligns the necessary resources to facilitate an on-time completion of your final report.

PCI DSS Compliance Mapping With MSS

10.2 REQUIREMENT 10.2 Automate & Verify

Implement automated audit trails for all system components to reconstruct the following events:

- **10.2.1** Verify all individual access to cardholder data is logged.
- **10.2.2** All actions taken by any individual with root or administrative privileges.
- **10.2.3** Verify access to all audit trails is logged.
- **10.2.4** Verify invalid logical access attempts are logged.

10.4 REQUIREMENT 10.4 Record

Record at least the following audit trail entries for all system components for each event:

- **10.3.1** User identification
- **10.3.2** Type of event
- **10.3.3** Date and time
- **10.3.4** Success or failure indication
- **10.3.5** Origination of event

10.5 REQUIREMENT 10.5 Audit Trails

Secure audit trails so they cannot be alter:

- **10.5.1** Limit viewing of audit trails to those with a job-related need.
- **10.5.2** Protect audit trail files from unauthorized modifications.
- **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

10.6 REQUIREMENT 10.6 Daily Review

10.6.1 Review the following at least daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions.
- **10.2.4** Verify invalid logical access attempts are logged source.