

## CLIENT NEEDED TO BECOME PCI-DSS COMPLIANT



### CHALLENGE

A large organization with numerous data entry points and users, this organization is an ever-changing repository of personal and other data. With so many users, and the reliance on credit cards for payment, there were concerns around loss of data, security breaches, and PCI conformity. While a large, talented internal IT team was in place, there was no specific skill set capable of determining what needed to be done, and how to assure senior management that they would be PCI compliant in time.

### SOLUTION

A consulting engagement employing Graycon senior security experts were engaged to:

- Improve the security posture at the client's site until an Information Security Manager was hired.
- Work with the client identifying and defining work that Graycon resources would take ownership of in an effort to address security remediation steps identified in Graycon's Security Assessment Report.
- Provide information security and PCI expertise as needed to support the client's information and technology security requirements as needed within this project.
- Ensure efforts towards PCI Compliance are in accordance with the latest PCI standards.

### RESULT

Graycon completed the Security Assessment Report and with the internal team immediately shored up smaller issues before assuming control of the larger, remediation concerns.

- Analysis of gaps from the PCI Self-Assessment Questionnaire (SAQ) were presented
- All gaps outlined in the completed version of the PCI SAQ were prioritized then remediated.
- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- The institution is now secure and PCI Compliant

**Stability**  
**Structured Approach**  
**Secure**  
**PCI-DSS Compliant**