InfoSight Enterprise Security Solutions for PCI-DSS

As a part of the PCI compliance process, most organizations are wise to assess their readiness prior to an official audit. It is an extremely valuable exercise that puts your organization in the best possible position for a successful audit and a sound security program. But finding vulnerabilities is only the first step toward addressing associated risks. **Addressing your vulnerabilities and security risks and developing a sound remediation roadmap is arguably the most critical step in the process.**

InfoSight can assess your, IT Security, Network Infrastructure, Applications, Policies and Operational Procedures to help you identify potential gaps between your current security posture and PCI requirements. **An effective way to discover vulnerabilities is to combine a Risk Assessment with Vulnerability Scanning and Penetration Testing**. Each of these activities plays a vital part in building a risk profile of your organization. Upon completion, you'll understand:

- How much of your data falls under PCI guidelines
- Which information is most at risk
- How difficult it is to obtain data from both inside and outside your network
- Who potentially can access your stored credit card data
- What remediation measures should be taken to protect your assets

InfoSight can provide an initial **PCI Security and Gap Analysis with the findings, recommendations, and a prioritization of remediation activities**. Additionally, we can provide a compliance roadmap, leading to relevant scoping and assistance with your Self-Assessment Questionnaires (SAQs).

Moving forward, InfoSight can assist with ongoing **24X7 Security Monitoring and Penetration Testing to ensure future compliance**. Proactively testing your security measures on an annual basis is one of the most important things you can do to protect customer account data, validate compliance and ensure a sound security posture. InfoSight provides many services and solutions including:

- **Vulnerability Assessments & Penetration Testing:** Assessments and testing to identify current application and network-based weaknesses and vulnerabilities prioritized by severity.
- **GAP Analysis & Compliance Roadmap:** Discover which requirements are being met and which are not. Measure the investment of time, money and resources needed to comply with PCI-DSS
- **Scoping Assistance:** Determine what system components are governed by PCI-DSS. In-depth discovery for accurate compliance and reduced liability. Identify and track all locations and flows of cardholder data in order to secure it, as well as to limit the scope of the audit to relevant systems only.
- **Self-Assessment Questionnaire (SAQ) Assistance:** Assistance selecting the SAQ and attestation that best applies to your organization and strategies in preparing for compliance validation. The SAQ is a validation tool for eligible organizations who self-assess their PCI-DSS compliance and who are not required to submit a Report on Compliance (ROC).

- **Remediation Assistance:** Assistance mitigating vulnerabilities in Web Applications, databases and files
- **Secure Network & Systems Design:** Prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Define the architecture, components, modules, interfaces, and data so you can incrementally address PCI requirements according to your business and technical priorities.
- **Wireless Analysis:** Ensure a well-designed and optimally performing wireless network. Analyze and monitor the wireless network from the wireless network edge all the way to the data center.
- **Compliance Assurance Program:** Comprehensive audit of all access to cardholder data to reduce the number of vulnerabilities and the associated risk of data compromise. Ensures the provisions of regulatory guidelines are being met

Many organizations are not aware of their responsibilities when it comes to PCI compliance. They think that this is somebody else's responsibility - like a vendor or credit card payment processing company. However, all parties involved in handling, processing and storing a credit card and credit card holder information have shared responsibilities. The ultimate responsibility in a hotel or restaurant, for example, lies with the operator.

13 Compliance Requirements

The PCI-DSS compliance is important to protect guest's person information and prevent your property from being penalized by the payment card industry. **The PCI DSS 13 requirements to meet compliance are:**

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks requirement
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications requirements
7. Restrict access to cardholder data by business need-to-know.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security