

PCI DSS Gap Analysis and Compliance Audit

Our PCI DSS Gap Analysis is designed to help a company determine where gaps in its security infrastructure are, prior to a full PCI DSS risk assessment. Our assessment services identify and scope the requirements for PCI compliance as it relates to the company, its agencies, merchants and services providers.

Our scanning services allow you to identify vulnerabilities that may block your company from meeting the PCI security requirements. Our reviews of education and training of all stakeholders, network architecture, plus network and application security procedures will provide a solid foundation of recommendations that will allow you to anticipate issues that may arise in a full SAQ or QSA review.

How the process works:

- Identify gaps in operational procedures
- Identify gaps in policy documentation
- Identify technical vulnerabilities

Key value propositions include:

- Quickly validate problems and resolution, prioritize vulnerabilities
- Automated testing provides recommendations for remediation
- Discovery of key weaknesses policies and procedures
- Categorize missing controls
- Review of network, operating system, application and end-point security measures
- Development of key remediation recommendations






BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge Transfer

FEATURES & BENEFITS

- Simulates a PCI SAQ assessment
- Consistent and repeatable testing
- Comply with industry-driven regulatory requirement
- Anticipate problems in a full PCI DSS assessment
- Fixed fee

PCI DSS Gap Analysis and Compliance Audit Steps

Steps	Enterprise Level
Automated Security Scanning: Commercial scanning tools used to identify potential vulnerabilities.	
Report Development and Interpretation: Recommendations report to fix gaps that would impact a PCI security assessment.	
Network Architecture Review: Review network security design and identify weaknesses.	
Security Policy Review: Review up to 10 security policies for gaps in procedures.	
Automated Security Re-Scan (within 3 months): Re-scan identified systems after patches are put in place.	

Ready To Get Started?

Contact us at **888-282-0696** or sales@aurorait.com to learn how Aurora Security Services can help you accomplish your specific business and IT security goals. Explore further by visiting our website at: www.aurorait.com