

{Information Security Audit & Assessment}

Information is one of an organization's most important assets. Protection of information assets is necessary to establish and maintain trust between the organization, its partners, and its customers. Timely and reliable information is necessary for an organization to operate and make decisions. An organization's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

A strong security program reduces levels of reputation and strategic risk by limiting the organization's vulnerability to intrusion attempts and maintaining confidence and trust in the organization. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services.

igxglobal can aid a client in achieving a sound Risk Management and Information Security Program through its Information Security Audit and Assessment offering. The purpose of this assessment is to conduct a thorough analysis of an organization's Information Security Posture. The analysis is designed to determine an orga-

nization's current security posture, its compliance to regulations (HIPAA, GLBA, SOX404, CJIS, PCI) and laws (State and Federal) as they pertain to the organization's industry, and to discover possible vulnerabilities and weaknesses within the current information security program.

igxglobal's Information Security Audit and Assessment, combined with our External Vulnerability/Exploitation Assessment, can provide an organization a complete picture of its current Information Security state, providing guidance and recommendations to mitigate and fill any discovered gaps, which thereby allow an organization to avoid possible penalties and fees associated with non-compliance.

igxglobal has been a focused provider of security services, such as the audit and assessment practices and compliance GAP analysis (HIPAA, GLBA, etc.), since 2000. In 2006, igxglobal, Inc. was approved by Visa and the Payment Card Industry as a certified PCI Data Security assessor.



SECURITY OPERATIONS



THREAT MITIGATION



SECURITY TECHNOLOGIES



PROFESSIONAL SERVICES



INFORMATION SECURITY/AUDIT & ASSESSMENT

igxglobal's Information Security Audit & Assessment includes the following:

- Policy and Procedure Review
- Active Social Engineering
- Third Party Oversight Review
- System Inventory and Documentation Collection
- Physical/Environmental Security Review
- Personnel and IT Staff Training and Awareness Review
- Internal Vulnerability Assessment
- Host/Network Diagnostic Review
- Access Control Review
- Data Flow and Network Usage Analysis
- Wireless Network Security Analysis
- Testing of Deployed Security Measures
- Monitoring/Response Process Assessment

Upon completion of the Information Security/Audit & Assessment, a report is provided that details the following:

- Copies of collected notes, raw data, and raw logs collected during the course of the assessment
- Summary of what information needs to be protected and the implications if it is damaged or lost
- Recommendations for addressing data flow and network usage security issues
- Summary of an organizations monitoring and response program and its effectiveness on outside sources
- A risk rating of existing vulnerabilities and exploits
- Summary of security measures in place and their effectiveness in securing the network and minimizing intrusions and vulnerabilities
- Identification of network security best practices and identity needed technology, policies, etc. to provide a secure environment
- Details on all client systems connected to the networks that are discovered in the course of the engagement, including all information discovered about those systems (i.e. operating system, available services, version information, etc.)
- Recommendations for enhancements in regards to overcome potential physical vulnerabilities
- Recommendations for heightened awareness and additional training
- A detailing of all security findings and existing vulnerabilities to include a detailed analysis of the vulnerabilities, potential risk they present to the systems and the network, and regulatory compliance
- A prioritized list of vulnerability mitigation recommendations rated from high to low
- Identification of network strengths and areas of improvement and where appropriate correlated with affected regulations
- Cost analysis for mitigation steps to improve security