

Security Auditing Services by Agilon

Today's information security climate goes beyond the traditional fears of compromise by hackers and viruses running. Government regulations such as Sarbanes-Oxley, HIPAA, and California SB1386 have become major drivers for organizations to revisit their computer and network security approaches. Partner-driven requirements such as Visa's CISP and MasterCard's SDP are putting additional pressure on organizations to have a strong set of controls around critical data. Building a solid security foundation is paramount to protecting your data and your donors.

A security program must encompass not only technology, but also people and processes. In fact, it is only once the program has been developed in terms of people and processes that it can be determined what technologies are appropriate to serve the security goals of an organization. It is critical that the requirements of an organization drive security technology, not the other way around.

Agilon has developed a comprehensive program for auditing and assessing the security environment surrounding your critical information systems. Based on the international standards established by ISO/IEC 17799:2000, and the Payment Card Industry (PCI) Data Security Requirements, our security auditing services are tailored to the operational needs of fundraising organizations.

Security Auditing Service Overview

Agilon's security auditing services are designed to meet the needs of nonprofit fundraising organizations. Through a combination of on-site audits of your computer systems' configuration, your organization's policies and procedures, together with automated testing of your systems to identify potential vulnerabilities, we provide you with a comprehensive assessment of your current security environment, and specific recommendations to correct any potential weaknesses that may be found. Key areas of the audit are:

- External Network Audit:** Taking an outsider's view of the network and seeing what is in place, and how it is configured, including quarterly network scans to identify potential vulnerabilities.
- Internal Network Review:** Assessing the critical aspects of how security is implemented and enforced by your internal computing systems.
- Policy & Procedure Review:** Security policies and procedures are the foundation of a secure network. Content, communication and enforcement are key to maintaining a security program.
- Analysis & Reporting:** The audit report is a collective summary of how the network is currently operating, and what risk, and where improvements need to be made.



**Protect Your Data...
... Protect Your Donors**

SECURITY AUDIT PROFILE

Phase 1 – Planning

The planning phase consists of mostly gathering basic information about the environment, as well as establishing boundaries and limits for the system analysis and test activities. The information provided for the planning phase is gathered using a structured site survey document completed by the customer.

Phase 2 – Testing

The testing phase is the time during which the actual audit is performed, in depth. The scope of the testing varies depending on the engagement, but is established during the planning phase. The possible areas of review include:

External Network Review - Taking an outsider's view of the network and seeing what is in place, and how it is configured. Aspects covered during an external review are:

- Firewalls & Routers
- Perimeter devices
- VPN connections
- Web and FTP servers
- E-mail servers
- Remote access methods

Internal Network Review - An often overlooked and very critical aspect of network security. Areas of the internal review include:

- Users accounts & password policies and practices
- Access privileges and levels
- File, directory, event log and registry permissions
- Audit logs
- Software Patch management
- Physical network cabling
- Backup methodology & disaster recovery plans

Policy Review - Security policies are the foundation of a secure corporate network. They must exist, be enforced, and be kept up to date. To help ensure this, the security audit covers:

- Business drivers of the security policy
- Information security roles and responsibilities
- Physical security
- Authentication and network security
- Internet and e-mail security policies
- Intrusion detection and virus scanning
- Encryption policy
- Policy content and enforcement
- Use of resources
- Incident reporting and response
- Disaster recovery plan

Phase 3 – Analysis & Reporting

The audit report is a collective summary of how the computer systems and network are currently operating, identifying potential security risks, and recommending changes and improvements. The detailed security audit report provides actionable direction for mitigating information security risks and achieving compliance with applicable regulations and industry best practices.