

Standards compliance protects your data integrity and network assets

If you rely on your IT infrastructure to maintain data integrity and protect your business from financial losses, it's a good idea to invest in network monitoring and maintenance, and achieve compliance with legislated standards.

GRH Consulting, LLC., plays an important role in helping you achieve standards compliance and maintain the integrity of your IT infrastructure. Figuring out how to comply doesn't have to be complex and expensive. We're already familiar with the standards and our complete managed services model enables us to quickly identify any areas of your IT network that are not yet up to standard.

To assess your level of current compliance, we'll conduct a non-intrusive network audit. The audit focuses on the seven key areas listed below, and is a great way to establish a baseline for making improvements.

These seven areas (known as SAS70) have been defined by the American Institute of Certified Public Accountants.

IT Requirement	GRH Consulting, LLC Advantage
Controlled Environment	Best Practices, Network Health Monitoring, Roles and Permissions Management, 24x7 Monitoring, Patch Management
Physical Security	SNMP-based Monitoring, Event Logging, Asset Discovery
Disaster Management	Readiness Planning via Reports, Performance Monitors, Backup Management, Collaborative Services
Availability	Continuous Monitoring, Remote Management, Deep Monitoring of Critical Servers
Information Security	ISO17799-Compliant Solution, Password Controls, Auditing, Intrusion Detection, Vulnerability Assessment
Network Security	Firewall Management, MBSA Integration
Network Health Visibility	Summary Reports, Asset Inventory, Capacity Planning, Customer Dashboards

From an IT perspective, compliance regulations ensure accurate disclosure of risk to investors and safeguard misuse of personal information. Companies must have effective processes in place that focus on security, privacy and assessment of risk. The other side of this page lists the most prominent legislative acts that have direct impact on IT management and how GRH Consulting, LLC., can help.



Act Name and Description	Applies to...	GRH Consulting, LLC Role
<p>Sarbanes-Oxley (Sarbox)</p> <p>Manage a secure and controlled infrastructure for data, processes, and historical information.</p>	<p>Global Public Companies</p>	<p>Security, Risk Management</p> <p>Monitoring for security, virus protection, intrusion detection, vulnerability management, and user authentication. Asset management and error logging for audit trails.</p>
<p>Gramm-Leach-Bliley (GLBA) and The New Capital Accord (Basel II)</p> <p>Implement systems for security and authorized access, and build safeguards against threats and hazards.</p>	<p>Global Finance Sector</p>	<p>Security, Patches, Planning</p> <p>24x7 monitoring for security breaches and vulnerabilities using industry security standards. Alerts, patch management and remote management help ensure network availability.</p>
<p>Federal Food & Drug 21-CFR-11(21-CFR-11)</p> <p>Ensure security, integrity, and availability of information. This is of particular concern to the health care industry that relies on the accuracy of patient / product information.</p>	<p>US Healthcare Sector</p>	<p>Security, Availability</p> <p>Secure environments and authenticated users. Reports indicate overall network health and help ensure the availability of data.</p>
<p>Payment Card Industry Data Security Standard (PCI-DSS)</p> <p>Ensures network standards to reduce vulnerabilities, and protect cardholders from fraud. Five goals: maintain secure networks; protect transaction data; reduce vulnerabilities; implement strong access control measures; and regularly monitor and test networks.</p>	<p>Global Credit Card Merchants</p>	<p>Security, 24x7 Monitoring</p> <p>Managed Workplace provides a Central Dashboard to monitor 24x7 any intrusion, or authorized access, as well as system failures that could impact prompt response.</p>
<p>Notification of Risk to Personal Data Act (NORPDA – US 2003), European Data Protection Directive (EUDP)</p> <p>Ensures that an agency notifies individuals if their personal information has been acquired by an unauthorized source. The impact to IT is to improve security and reporting systems.</p>	<p>US and Europe Any company</p>	<p>Security, Monitoring</p> <p>We can instantly detect and warn about unauthorized access. Remote management allows for rapid action against intrusion. Patch management ensures up-to-date system security.</p>
<p>The Health Information Portability & Accountability Act (HIPAA)</p> <p>Ensures patient record privacy by improving IT security and interoperability of information systems, as well as improved reporting systems.</p>	<p>US Healthcare Sector</p>	<p>Privacy, Availability, Reporting</p> <p>Best-in-class tools to ensure security and availability of network systems, as well as protecting them from unauthorized entry.</p>
<p>Personal Information Protection & Electronic Documents Act (PIPEDA)</p> <p>Balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.</p>	<p>Canada Any company</p>	<p>Privacy, Reporting</p> <p>Best-in-class tools to ensure security and availability of network systems, as well as protecting them from unauthorized entry.</p>