



# Addressing Regulatory Compliance in the Healthcare Industry

January 2006

---

## Contents

<b>Healthcare Industry Overview</b>	<b>1</b>
<b>Healthcare Industry IT Regulations.....</b>	<b>3</b>
<b>NetIQ Products Offer a Compliance Solution .....</b>	<b>5</b>
<b>Achieving Compliance with NetIQ .....</b>	<b>7</b>
<b>How NetIQ Security Products Can Help.....</b>	<b>10</b>
<b>About NetIQ Corporation .....</b>	<b>16</b>

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is probably the first regulation that people think of when considering healthcare in the United States. However, organizations within the industry may be subject to many additional regulations.

This paper is concerned with the organizations that provide services to consumers within the United States Healthcare industry and how existing regulations affect the management of information technology resources within those organizations. It also demonstrates how NetIQ can help organizations comply with those regulations.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

**© 1995-2005 NetIQ Corporation, all rights reserved.**

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, imMarshal, Intergreat, Knowledge Scripts, MailMarshal, Marshal, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Security Reporting Center, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebMarshal, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

# Healthcare Industry Overview

The United States Healthcare industry covers a wide range of healthcare participants, from providers to pharmacists to insurers to the patients themselves. Organizations within the industry may be subject to a multitude of regulations and must ensure compliance with all relevant regulations to avoid potential fines. The applicability of a regulation to an organization depends on many factors, including the size of the organization, whether it is publicly traded, or if it is a federal agency.

The respect for privacy has been embedded within the medical profession since the creation of the Hippocratic Oath, one of the oldest binding agreements in history. Today, graduating medical students in medical schools worldwide swear to this oath, including nearly 100% of U.S. medical schools. The top drivers for doctors are to provide care, meet their ethical and professional obligations, and work successfully within their environment.<sup>1</sup> However, doctors are only a part of the industrial machine that is healthcare, and organizations and other individuals that operate within its boundaries are not subject to the Hippocratic Oath.

This paper examines the key business trends in the healthcare industry, and examines how IT is being increasingly used to satisfy drivers originating from regulatory compliance, cost control and customer satisfaction. The paper then discusses the major regulations that affect the industry, and highlights the areas of those regulations that may apply to organizations within healthcare. Finally, it will be shown how NetIQ can assist customers with both its solutions and methodology to address the compliance requirement of healthcare, as well as ensuring that risks are effectively managed and that the assets of the organization remain secure.

## Key Business Trends in Healthcare

In Table 1 are shown the key drivers for organizations within the healthcare industry, which vary slightly between those providing the care and those paying for the care. Common elements can be clearly identified within the two groups. For example, both are concerned with being in compliance with governmental regulations, and many will be subject to additional scrutiny due to their outsourcing contracts, especially around the issues of privacy, security, risk, and business continuity associated with increased offshore outsourcing.

Healthcare Provider Drivers	Healthcare Payer Drivers
Compliance With Government Regulations	Consolidating Market
IOM <sup>1</sup> Report/Medical Error Reduction	Aging Population
Desires to Cut Healthcare Costs	Increasing Regulations (such as HIPAA <sup>2</sup> , SOX <sup>3</sup> )
Competitive Differentiation	Competitive Differentiation
Cost-reduction/Operational Efficiency	Cost Reduction/Operational Efficiency
Improving Reimbursement	Consumers as a “New Customer”

**Table 1 North American Healthcare Market Drivers by Segment<sup>ii</sup>**

<sup>1</sup> Institute of Medicine

<sup>2</sup> U.S. Health Insurance Portability and Accountability Act

<sup>3</sup> U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002

Related to the above is the cost of ensuring compliance. Some have estimated that HIPAA compliance costs 33 cents of every health care dollar that was spent between 1996 and 2002. Gartner identified security for privacy compliance as one of the top 10 issues within healthcare in 2003, and an area that is misunderstood and the cause of significant spending by healthcare organizations. This spending is one of the areas healthcare organizations wish to control, especially when considering that health care costs have suffered a double-digit rise during the past three years. By year-end 2004, 70% of healthcare organizations with annual budgets greater than US\$100 million are using HIPAA-compliant claims and remittance advice; by year-end 2005, half of all care-delivery organizations that have not upgraded their patient accounting software to meet HIPAA requirements will be forced to submit paper claims to at least two of their major payers.

In the United States, 45% of healthcare services are purchased through government health plans such as Medicare and Medicaid.<sup>iii</sup> Medicare and Medicaid, which are today managed by the Centers for Medicare and Medicaid Services (CMS), were created by the Social Security Act of 1965 as federal health insurance programs providing healthcare coverage for the elderly, the disabled, and the indigent of all ages. To become certified, providers must satisfy the requirements of: being financially solvent; complying with Title VI of the Civil Rights Act of 1964, which prohibits discrimination; and meeting the program's conditions of participation. These weak requirements have led to many organizations being created that are now suffering the nightmare of compliance with regulations.

## Key IT Trends in Healthcare

A key goal of many healthcare organizations, especially those run by federal agencies (which are subject to many additional regulations), is to utilize information technology to manage information internally, to share information between parties and to also reduce costs. Customers also expect an increased ability to access their health and benefits information via the Internet, driving organizations in the healthcare industry to cater to these expectations. After 2004, 90% of healthcare organizations will have executed at least one Web-based service intended to improve revenue cycle management, extended customer service and marketing functions, or reduced operating costs. Gartner suggests that providers must focus on automations systems to support their business strategy in order to meet the following goals for 2004<sup>Error! Bookmark not defined.</sup>:

- Improve operational efficiency
- Increase access to information internally and externally
- Support customer/consumer-focused initiatives

However, the costs associated with this continual move to electronically-based information are forcing the healthcare industry to increase its spending on IT, an amount that is expected to grow at a compound annual growth rate (CAGR) of 7%, from US\$34.1 billion in 2001 to US\$47.9 billion in 2006. Of this spending, security will be taking a large chunk of the pie. Through 2005, despite HIPAA and media attention on cybersecurity, U.S. healthcare spending on security will grow at a CAGR of 10% or less; through 2005, 80% of expenditures on information security by healthcare organizations will be for solutions to define, manage and monitor the legitimate use of information systems by authorized users.

---

# Healthcare Industry IT Regulations

There are a myriad of regulations affecting the healthcare industry, depending upon whether you are a public company, private company or federal agency. This section provides an introduction to this constantly evolving space, in which organizations must examine not just federal regulations, but also state regulations (which may override federal guidelines).

## Health Insurance Portability and Accountability Act of 1996

All healthcare organizations are affected in some way by HIPAA. The entities that are affected include all healthcare providers (even one-physician offices), health plans, employers, public health authorities, hospitals, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations and universities.

The rules of HIPAA are published by the Department of Health and Human Services (HHS) and enforced by the Centers for Medicare and Medicaid Services (CMS) and the Office of Civil Rights (OCR). While the provisions stated in the Act, they can be overridden by laws created by individual states, meaning that healthcare organizations need to be conscious of both federal and state government laws in this area.

HIPAA calls for severe civil and criminal penalties for noncompliance, including:

- Fines up to \$25,000 for multiple violations of the same standard in a calendar year
- Fines up to \$250,000 and/or imprisonment up to 10 years for known misuse of individually identifiable health information

The two main rules of HIPAA are:

- **Privacy Rule:** Organizations must identify the uses and disclosures of protected health information (PHI) and put into effect appropriate safeguards to protect against an unauthorized use or disclosure of that PHI. When material breaches or violations of privacy are identified, the organizations must take reasonable steps to solve those problems in order to limit exposure of PHI.

Compliance with HIPAA's PHI guidelines was required of all covered entities, regardless of size, by April 14, 2004.

- **Security Rule:** Defines the administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information. Covered entities are required to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion and transmission. The final rule states that all covered entities, with the exception of small health plans, must be compliant by April 21, 2005. Small health plans must be compliant by April 21, 2006.

## Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley Act) of 2002

The Sarbanes-Oxley Act of 2002 requires executive-level management of publicly traded companies to personally verify and sign the financial statements (and other related information) concerning the company they manage. Signed by President George W. Bush on July 30, 2002, the Act required large corporations to be compliant by June 15, 2004. Small corporations must be compliant by June 15, 2005.

From an IT perspective, the Act mandates that chief executives be able to verify that they have adequate “internal controls” to ensure that systems containing and working on the data that they eventually sign off on are secure. Implementation requirements are not specified in the Act, but left to the discretion of the organization to determine which controls are required to ensure the security of their systems and data.

## **Financial Modernization (Gramm-Leach Bliley) Act of 1999**

The Financial Modernization Act of 1999, more commonly known as the Gramm-Leach Bliley Act (GLBA), is designed to protect the personal financial information of consumers where stored by financial institutions. Such institutions are not limited to just banks or securities firms, but include any company that offers financial products or services to individuals, including insurance, credit and loans. In the healthcare industry, many organizations run some credit scheme or provide insurance and, as such, are subject to the regulations defined within GLBA.

Enforced by numerous federal entities, including the Federal Trade Commission (FTC), the Act requires compliance as stated in its two main rules: the Financial Privacy Rule and the Safeguards Rule.

- **Financial Privacy Rule:** Governs the collection and disclosure of consumer personal information, requiring organizations to provide consumers with privacy notices that explain how that organization uses and distributes their information. Through opt-out rights, consumers are also provided a degree of control over whether their information can be shared.
- **Safeguards Rule:** Requires organizations to design, implement and maintain safeguards to protect personal information.

## **Visa Cardholder Information Security Program (CISP)**

The Visa Cardholder Information Security Program (CISP) was announced by Visa in April 2000 and mandated June 2001. All merchants or service providers must have submitted their compliance documentation by September 30, 2004. All entities that store, process or transmit Visa cardholder data are required to comply with CISP and are also responsible for ensuring the compliance of their merchants or agents. Where organizations fail to comply, Visa may fine them up to \$500,000 per incident.

Visa’s CISP requires organizations to implement security to comply with 12 basic security requirements, including implementation of appropriate physical controls, logical controls and the performance of regular audits. The program also requires organizations to immediately report security incidents, as well as be able to investigate and take appropriate action to limit exposure of cardholder information. When the organization is in compliance, they will be automatically indemnified against any fines.

## **The PATRIOT Act of 2001**

The PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001, Public Law 107-56, was passed in response to a series of serious terrorist attacks against the United States. It provides greater power to federal law-enforcement and intelligence agencies in the area of surveillance with the goal of counteracting terrorist activities. In addition, through Section 1016 of the Act, it focuses upon the requirement to establish policies and procedures to protect the “critical infrastructure” of the United States, which it further defines as “systems and assets” —both physical and virtual— “that would have a debilitating impact upon security, the economy, or national public health or safety.” Also stated in the Act is that any disruption to the

critical infrastructure should be rare, brief, geographically limited in effect, manageable and display a minimally detrimental effect. The impact on healthcare organizations is that, as a piece of the puzzle that provides national public health, they must establish mechanisms to protect their infrastructures and be in compliance with the requirements of the Act.

## Privacy Act of 1974

The Privacy Act of 1974 (5 USC Section 552a) protects individuals by giving them the right to determine the extent to which their personally identifiable information may be distributed, as well as the ability to gain access to their records and have corrections made if required. Where organizations collect personally identifiable information that is then stored on information systems under their control, they may only store such information that is absolutely necessary. At time of collection of this information, individuals must be informed of their rights under the Act, as well as the purposes for which the information will be used.

---

## NetIQ Products Offer a Compliance Solution

The healthcare organizations that maintain electronic patient information must ensure the privacy and confidentiality of that information by complying with regulations discussed above. NetIQ security and administration products help health care organizations comply with these regulations.

Three categories of requirements for safeguarding patient information comprise the HIPAA security standard, and which neatly satisfy the requirements of other regulations, are:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

## Administrative Safeguards

The Administrative Procedures deal with defining and implementing a security policy for keeping information private. The following table outlines the NetIQ products that help with administrative procedures.

Requirement	NetIQ Products to Address Requirement
Security Management ✓ Risk Management ✓ Sanction Policy	NetIQ Risk & Compliance Center, VigilEnt Policy Center, NetIQ Vulnerability Manager,
Assigned Security Responsibility	VigilEnt Policy Center
Workforce Security ✓ Termination Procedure ✓ Access Authorization ✓ Access Establishment & Modification	VigilEnt Policy Center, Directory and Resource Administrator, Directory Security Administrator, File Security Administrator, Change Guardian for Active Directory
Security Awareness & Training ✓ Security Reminders ✓ Log-in Monitoring ✓ Password Management	VigilEnt Policy Center, NetIQ Security Manager, NetIQ Vulnerability Manager, NetIQ Group Policy Guardian, Secure Password Administrator

Security Incident Procedures – Response and Reporting	VigilEnt Policy Center, NetIQ Security Manager, NetIQ Group Policy Guardian
Contingency Plan	VigilEnt Policy Center
Evaluation	VigilEnt Policy Center, NetIQ Vulnerability Manager
Business Associates Contracts and Other Arrangement	VigilEnt Policy Center

## Physical Safeguards

The Physical Safeguards deal with methods you use to protect data. The following table outlines the NetIQ products that help with physical safeguarding of data.

Requirement	NetIQ Products to Address Requirement
Facility Access	VigilEnt Policy Center
Workstation Use	VigilEnt Policy Center
Workstation Security	VigilEnt Policy Center, File Security Administrator, NetIQ Vulnerability Manager
Device and Media Controls	VigilEnt Policy Center

## Technical Safeguards

Technical Security Services and Technical Security Mechanisms deal with the methods you use for securing data access. The following table outlines the NetIQ products that help with technical security services and mechanisms.

Requirement	NetIQ Products to Address Requirement
Access Controls <ul style="list-style-type: none"> <li>✓ Unique User Identification</li> <li>✓ Emergency Access Procedure</li> </ul>	VigilEnt Policy Center, Directory and Resource Administrator, Directory Security Administrator, NetIQ Group Policy Administrator, File Security Administrator
Audit Controls	VigilEnt Policy Center, Directory Security Administrator, File Security Administrator, NetIQ Vulnerability Manager, NetIQ Security Manager, Directory and Resource Administrator, NetIQ Group Policy Guardian
Integrity	VigilEnt Policy Center, File Security Administrator
Person or Entity Authentication	VigilEnt Policy Center
Transmission Security	VigilEnt Policy Center

## Privacy Safeguards

Ensuring that the privacy of data is maintained is a requirement within many of the regulations that apply to the industry. For example, both HIPAA and the Privacy Act of 1974 require organizations to manage access to and modification of this private information by both authorized entities and the subjects of that data. Since private information can show up in so many different places and in so many forms, this places a tremendous administrative burden on organizations within the healthcare industry. NetIQ products can assist in the following ways:

Requirement	NetIQ Products to Address Requirement
Employee Training and Certification	VigilEnt Policy Center
Controlling Employee Access to Private Information	Directory and Resource Administrator, File Security Administrator, Change Guardian for Active Directory
Reporting Employee Access to Private Information	File Security Administrator
Monitoring Disclosure of Private Information in E-mail (both externally and internally bound)	VigilEnt Policy Center

## Achieving Compliance with NetIQ

To assist customers in achieving their compliance needs, NetIQ offers a five-step methodology for customers to assure compliance, reduce risk and secure assets. This methodology is presented in Figure 1. In each phase, NetIQ has the knowledge and resources available to assist customers in maximizing the effectiveness of their NetIQ products.

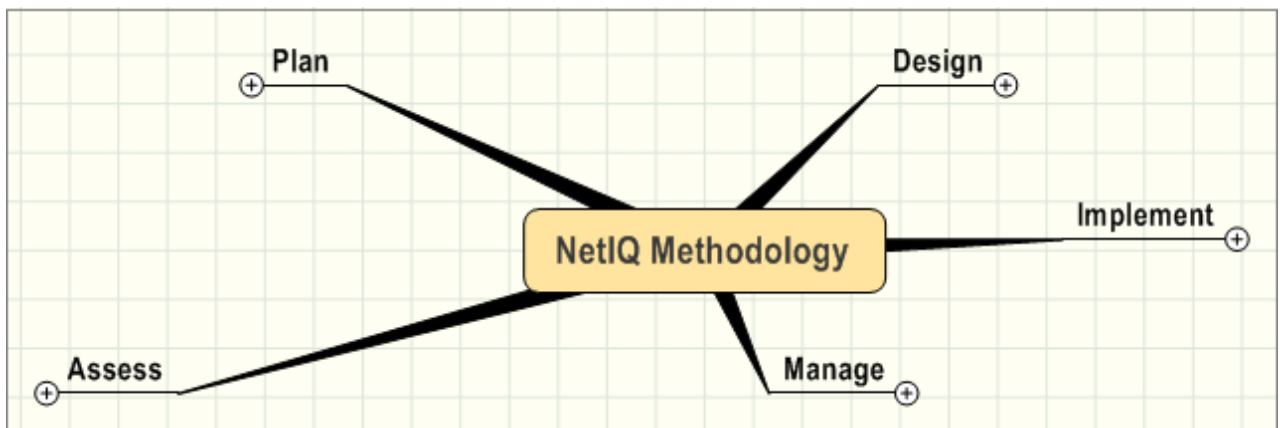
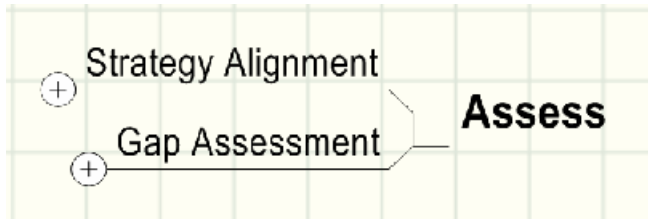


Figure 1 The NetIQ Methodology

### Assess

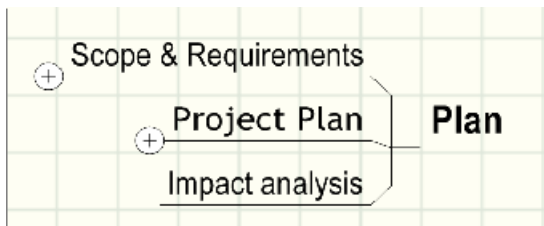


The initial step of the NetIQ methodology is to **assess** the current situation and parameters of the organization. This will create a baseline from which a plan can be put together, a design created and implemented, and then a program put into action for

effective ongoing management by the organization.

Assessment starts with determining the strategy of the organization and how different elements related to the operations of the business align with and/or affect that strategy. This involves looking at the objectives of the business, the industry and governmental regulations affecting that business, the risk drivers for the organization and the objectives for how IT is to be utilized within the enterprise. This ensures that the information security plan will be in alignment with the overall corporate business strategy.

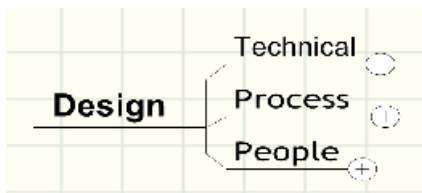
A gap assessment can then determine how well the IT operations currently align to the strategy goals of the organization. Policies are analyzed to determine how well they fit the strategic goals of the organization, as well as meet the requirements of industry and governmental regulations. Departmental procedures can then be examined to determine their fit with the corporate policies. In the same manner, technical controls can be investigated to determine how well they enforce compliance by both users and the automated system.



## Plan

Post-assessment comes the **planning** phase. Planning involves determination of the nature of the project, whether it is to assure compliance, manage risk or secure the corporation's assets. This is often the most critical phase of a project

since it sets the expectations and scope of the project, including the timeline, resources and dependencies that define the critical path to success. The key deliverable of this stage is the project plan, which is often supported by other materials including feasibility, scope and impact documentation.



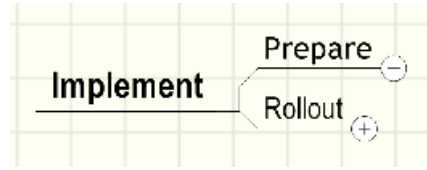
## Design

The **design** phase of the NetIQ methodology examines three key areas: technical controls, processes and people. The project requirements and knowledge of the organization are used to determine the required architecture.

If necessary, new processes are designed at this point or existing processes modified to ensure a successful implementation. Care is taken to ensure that the processes are also mapped to the technical controls, where appropriate for a cohesive design plan. The people side is also critical, requiring examination of those using, or being indirectly affected by, the system. Definition of

roles and the accesses permitted to each role, as well as determination of reporting requirements, will help the organization assure compliance with policies and regulations and ensure that their assets remain secure.

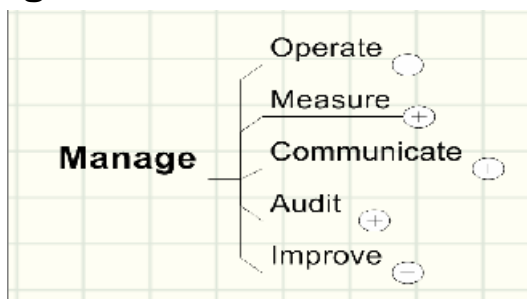
## Implement



The **implementation** phase involves the rollout of the system, including any preparatory work that needs to be completed. Through rollout of a new or updated system, organizations must deal with the operational concerns of running a staging environment, handling the running of

pilots and then being prepared for the complexities that can arise in the production environment. NetIQ can assist with the preparation of the technical environment, ensuring that products are configured to match the design plan and providing customization through product extensions and customized reporting. Full testing can then be carried out on staging systems, validating the movement into a pilot or production state and ensuring success of the project. While NetIQ products are designed to be simple to use, additional training can also be provided where required.

## Manage



The **manage** phase relates to the actual operations of a live system within the organization. The daily management of the enterprise infrastructure is in the hands of the operations staff of the business, which must constantly monitor the infrastructure, assess potential threats and respond in a timely manner. Senior management will expect communication of results, usually via simple reports, to ensure that compliance is successfully

enforced and that overall business risk is minimized. This regular review will ensure that when regulators perform audits upon the corporation, they will find full demonstration of due diligence and an effective security program that ensures compliance, reduces risk and ensures the security of the corporation's assets.

To optimize use of NetIQ products—such as correctly interpreting data, feeding knowledge back into the automated functions of the products or creating enhanced reporting—NetIQ offers additional training or on-site consulting to ensure that the organization realizes the maximum possible benefit.

---

## How NetIQ Security Products Can Help

### Security Policy Management

NetIQ Security Policy Management solutions help you manage security policies in a consistent, sustainable and automated fashion. This comprehensive approach ensures policies evolve to counteract the continuously adjusting landscape of regulations and threats. With built-in knowledge of the major compliance issues found in information security regulations, they help you in creating, distributing, testing and enforcing the security policies required by audits, regulatory acts and international standards.

NetIQ's solutions help you close the gaps between corporate security policies and the people who must practice and comply with these policies at a business, operational and technical level. NetIQ provides you with the most effective tools to create and maintain policies, educate people and enforce policy compliance across your entire organization.

Some key benefits of NetIQ Security Policy Management products are:

- ☑ Quickly and easily establish or adapt policies to fit your organization including specific regulatory and audit requirements, such as GLBA **Cardholder Security Programs**. Federal sector organizations that take or process credit card payments are likely subject to the cardholder security programs enforced by the payments vendors such as Visa and MasterCard. Both the Visa Cardholder Information Security Program and the MasterCard Site Data Protection Program require security controls and practices ranging from security management, security assessment, access controls, operations, monitoring and logging, and more. Each program also requires card merchants to undertake or be subject to annual security assessments.
- ☑ GLBA, HIPAA, and Payment Card Industry Data Security Standard.

- ☑ Educate users on policies quickly and effectively across your organization via web browser.
- ☑ Enforce acceptable Internet and email usage policies to improve efficiency, minimize security risks and limit legal liability exposure.
- ☑ Translate policies into practical and enforceable technical controls that can be easily implemented across the IT infrastructure.
- ☑ Make people your first line of defense, not your weakest link.

NetIQ Security Policy Management products enable you to:

- ☑ Easily create, review and approve policies online to expedite consensus and reduce time and effort.
- ☑ Communicate policies more effectively by providing online access in a user-friendly view that eliminates information overload and vastly improves comprehension, understanding and compliance.
- ☑ Measure and enforce policy compliance of users to assure they have read and understand all security policies relevant to their roles. Acceptable Use Policies for email, web browsing and instant messaging are automatically enforced to minimize the risk of lost productivity and security exposure.
- ☑ Measure, analyze and report the compliance of your critical systems to your stated policies, standards or leading practices.

### **NetIQ Vulnerability Manager**

<http://www.netiq.com/products/vsm/default.asp>

NetIQ Vulnerability Manager provides a fully integrated enterprise-class assessment solution for compliance with policies and standards, as well as the identification of vulnerabilities. NetIQ Vulnerability Manager leverages a flexible, scalable n-tier architecture to ensure minimal impact on your servers and network, with both agents and agent-less implementations possible. NetIQ Vulnerability Manager directly supports risk assessment and certification and accreditation (C&A) programs by generating scored checkup assessments of critical servers and workstations to ensure policy compliance, identify vulnerabilities and enumerate missing patches.

### **NetIQ Security Solutions for iSeries**

<http://www.netiq.com/products/iseries/default.asp>

NetIQ Security Solutions for iSeries provides simplified security auditing, vulnerability management and security administration that address the rigid regulatory mandates imposed on your iSeries enterprise. NetIQ also provides a comprehensive cross-platform enterprise security solution for OS/400, UNIX, Linux and Windows operating systems running on the IBM's flagship i5 midrange platforms.

### **VigilEnt Policy Center**

<http://www.netiq.com/products/vpc/default.asp>

NetIQ's VigilEnt Policy Center automates policy management best practices by enabling you to create security policies, distribute them online, educate employees and track and report compliance. VigilEnt Policy Center provides built-in expertise with more than 1,400 out-of-the box security policies and best practice standards that enable you to create, review, publish online, update and track compliance across the enterprise saving hundreds of hours of effort.

## Vulnerability Management

Your organization cannot completely eliminate risk from its environment, but you can intelligently and cost-effectively manage that risk. NetIQ Vulnerability Management solutions provide you with a true risk score for each of your IT assets, enabling you to determine what to protect and how much protection is needed. These solutions enable you to turn vulnerability management from a time-consuming project to a routine business process that leverages your existing staff and infrastructure.

NetIQ Vulnerability Management solutions also enable you to achieve balance and efficiency in risk management, by allowing you to decide how to manage your systems. These products offer fully customizable system groupings and profiles that enable assessment, auditing and patching of systems in the way that makes the most sense for the business needs of your organization.

Some key benefits of NetIQ Vulnerability Management products are:

- ☑ Continuously audit for policy exceptions, vulnerabilities and exposures using security configuration baselines based on policies, standards or best practices.
- ☑ Eliminate uncoordinated manual processes with centralized management and control.
- ☑ Provide metrics for security and compliance using scored assessments at every level of your business.
- ☑ Enhance the security of specific platforms and applications beyond their native capabilities, such as locking down network services on UNIX and iSeries and shielding web servers such as IIS and Apache.
- ☑ Deliver the broadest security solution available, enabling you to secure Windows, UNIX, Linux, NetWare and iSeries platforms - from operating systems to the web servers and databases that run on them.

NetIQ Vulnerability Management products enable you to:

- ☑ Ensure continuous policy and regulatory compliance so you can routinely audit systems to make sure they are configured according to company policy and stay that way. You can then evaluate compliance by business unit, geography, technology or other factors that are important to the organization.
- ☑ Efficiently perform vulnerability scans so you can scan all of your systems for a new vulnerability, and then incorporate the check(s) in regularly scheduled assessments to ensure they stay secure.
- ☑ Reduce risks with remediation management so once vulnerabilities have been found or critical systems have failed an audit, you can address these issues quickly and easily.

NetIQ's Vulnerability Management products include the following:

## **NetIQ Vulnerability Manager**

<http://www.netiq.com/products/vsm/default.asp>

In addition to providing policy compliance as described above, NetIQ Vulnerability Manager – as its name implies – provides enterprise-class vulnerability assessment and exploit identification. In order to keep pace with the latest vulnerabilities and threats, NetIQ has teamed with TruSecure to provide detailed knowledge on and checks for vulnerabilities and exploits through our AutoSync capabilities in NetIQ Vulnerability Manager. AutoSync provides a virtual pipeline for publishing and delivering vulnerability knowledge, as well as other security-related content, including patch databases, regulation templates and even sample policy templates. What makes NetIQ Vulnerability Manager unique is its ability to identify not only vulnerabilities and exposures, but also the symptoms or presence of exploits such as modified registry keys, infected files or other system changes.

## **Incident Management**

Keeping your IT systems secure in the face of constant internal and external changes can seem like an impossible task. NetIQ Incident Management solutions reduce the noise from managing multiple security applications and devices, respond automatically to resolve security incidents and deliver complete coverage across your enterprise IT infrastructure.

Some key benefits of NetIQ Incident Management products are:

- ☑ Identify breaches quickly and correlate incident information from popular third-party devices to properly manage incidents in a timely, efficient manner.
- ☑ Reduce false positives and event noise and expedite incident response and investigation.
- ☑ Automate the process of archiving logs and event data.
- ☑ Perform detailed analysis upon security data, including trend analysis and legal-strength forensics investigation.

NetIQ Incident Management products enable you to:

- ☑ Analyze events to comply with regulations, standards and policies using security log consolidation, retention, forensic and trend analysis, and historical reporting.
- ☑ Protect data with real-time host intrusion detection that assures server application availability, integrity and confidentiality.
- ☑ Correlate information from host and network intrusion detection systems, firewalls, antivirus software and other devices to reduce false positives, identify blended threats and reduce exposure.

NetIQ's Incident Management products include the following.

## NetIQ Security Manager

<http://www.netiq.com/products/sm/default.asp>

NetIQ Security Manager is a comprehensive security incident management tool that simplifies the management of security point products with real-time monitoring and alerting, advanced multi-stage correlation, analysis and automated response and reporting through a central security console. NetIQ Security Manager is unique in its seamless integration of three often disparate incident management technologies: multi-vendor security event management, host intrusion protection and heterogeneous log consolidation. These capabilities are provided by the following NetIQ Security Manager modules:

- ☑ Event Manager for NetIQ Security Manager centralizes the management of security devices and applications across the event lifecycle, including real-time monitoring, advanced correlation, forensic analysis and automated response and reporting.
- ☑ Log Manager for NetIQ Security Manager helps you meet audit and legal requirements with powerful real-time security log consolidation, analysis and reporting.
- ☑ Intrusion Manager for NetIQ Security Manager improves server and application availability and protects intellectual property with real-time, host-based intrusion detection and response.

NetIQ is unique in its ability to provide all three capabilities in a single, integrated product suite.

## Operational Change Control

NetIQ Change Control & Audit solutions assure that you can authorize, verify, audit and monitor changes across your IT environments. Through an automated approach, IT change management processes are reinforced with the knowledge and confidence that only authorized and intended changes have been implemented. With support for best practices, such as ITIL and COBIT, NetIQ Change Control & Audit solutions enable you to more easily comply with leading regulations—such as Sarbanes-Oxley and HIPAA—empowering you to:

- ☑ Centrally audit managed, unmanaged and high-profile Active Directory changes
- ☑ Alert on changes and prioritize according to their risk level and the level of importance of the change
- ☑ Know you are in compliance by utilizing out-of-the-box auditing templates designed to automate common compliance queries

NetIQ Change Control & Audit solutions enable you to:

- ☑ Gain control over change in you IT environment with powerful change monitoring reports and alerting capabilities.
- ☑ Assure service availability through the integration of NetIQ's Change Control & Audit solutions with your Change Management process.
- ☑ Automatically parse change audit reports using out-of-the-box templates for different audiences, such as auditors or management.

NetIQ's Operational Change Control products include the following.

### **Change Guardian for Active Directory**

<http://www.netiq.com/products/cgad/default.asp>

With NetIQ's Change Guardian for Active Directory, you know which changes are executed based on corporate policy, validate the success or failure of planned changes and capture the difference between authorized and unauthorized change activity. The Change Guardian product minimizes the risks associated with changes to Active Directory by assuring that changes to the production Active Directory environment are authorized, monitored, verified and audited through implementation.

### **Directory and Resource Administrator**

<http://www.netiq.com/products/dra/default.asp>

Directory and Resource Administrator provides advanced delegation and powerful, policy-based administration capabilities that dramatically reduce ongoing workload and costs while enhancing the security of your Windows environment.

### **Directory Security Administrator**

<http://www.netiq.com/products/dsa/default.asp>

NetIQ's Directory Security Administrator provides innovative Active Directory permissions management capabilities, which include powerful role-based security, auditing and advanced analysis.

### **NetIQ Group Policy Administrator**

<http://www.netiq.com/products/gpa/default.asp>

NetIQ Group Policy Administrator is the industry's leading solution for planning, managing, troubleshooting and reporting on Group Policies.

## **Unified Compliance Reporting**

Just as important as implementing the controls required by GLBA and other regulations, is the ability to communicate the status of those controls to management. Unified Compliance allows you to build and implement IT controls once, while reporting on those controls against the varying regulations your agency may face.

Some key benefits of NetIQ's risk and compliance reporting products include:

- ☑ Demonstrates regulatory compliance by mapping technical assessment results to specific regulations and standards to present compliance metrics for different control areas.
- ☑ Delivers on-going risk analysis, measuring IT security risk in your environment using innovative metric models based on compliance exceptions, vulnerabilities and the business value of IT assets.
- ☑ Centralizes security information for easier access and decision making by mining security assessment results reflecting system configurations, vulnerabilities, patch levels, user accounts and permissions, auditing and more.
- ☑ Turns complex data into easy-to-understand, actionable information via a customizable interface. Views can be tailored to your regulatory, organizational and technical needs.

NetIQ's Compliance Reporting products include the following.

### **NetIQ Risk & Compliance Center**

<http://www.netiq.com/products/rcc/default.asp>

The NetIQ Risk and Compliance Center solution aligns security metrics gathered from your IT systems to demonstrate compliance with IT related policies and regulations and displays them in a customizable dashboard. This automated solution analyzes security assessment data and maps the results with government and industry regulations, such as Sarbanes-Oxley, HIPAA and GLBA. As a result, it provides the knowledge you need to understand and manage ongoing security risks and build a defensible position to prove regulatory compliance to auditors.

The NetIQ administration products provide the best management and analysis products for your environment. These products automate administration tasks to avoid costly mistakes, enforce policies to maintain your security model, secure data on the network, report changes to permissions, analyze computer configurations and permissions, and automate group policy management.

With these NetIQ products, you can meet your compliance goals while streamlining your business processes and reducing your overall costs of doing business.

---

## About NetIQ Corporation

NetIQ is a leading provider of integrated systems and security management solutions that empower IT organizations with the knowledge and ability necessary to assure IT service. NetIQ's Knowledge-Based Service Assurance products and solutions include embedded knowledge and tools to implement industry best practices and to better ensure operational integrity, manage service levels and risk and ensure policy compliance. NetIQ's modular, best-of-breed solutions for Performance & Availability Management, Security Management, Configuration & Vulnerability Management, and Operational Change Control integrate through an open, service-oriented architecture allowing for common reporting, analytics and dashboards. We empower IT organizations with the knowledge of their IT service levels through automated assessment, understanding and real-time management of current configurations, known vulnerabilities and risk. With NetIQ you know your IT service is assured.

Headquartered in San Jose, Calif., with offices and development facilities in 16 countries worldwide, NetIQ employs 900 people and has more than 3,000 enterprise customers. For more information, please visit the company's web site at [www.netiq.com](http://www.netiq.com) or call (888) 323-6768.

---

<sup>i</sup> <http://csrc.nist.gov/nissc/2000/proceedings/papers/915slide.pdf>

<sup>ii</sup> M. Davis & J. Galimi, North American Healthcare IT Spending Forecasts to 2007, Gartner (24 April 2004)

<sup>iii</sup> J.Klein, Healthcare's 2004 Underlying and Emerging IT Client Issues, Gartner (13 November 2003)