



# The Fusion of Compliance and Risk Management

## White Paper

February 2007

---

### Contents

<b>Mandates for IT Compliance and Risk Management.....</b>	<b>3</b>
What Is Compliance? .....	3
Risk Management.....	5
<b>NetIQ's Methodology for Compliance &amp; Risk Management.....</b>	<b>5</b>
Policy Framework .....	6
Assess .....	6
Operate .....	9
Control.....	11
Metrics and Reporting .....	14
Pulling It All Together – NetIQ Risk & Compliance Center....	16
<b>About NetIQ Corporation</b>	<b>17</b>

Many IT departments and security officers strive to implement successful policy compliance programs. These programs are often designed to satisfy regulatory and audit-related requirements to protect the integrity of financial reporting or other critical information (e.g., pharmaceutical trial results, operational data) or prevent the loss of sensitive information (e.g., health information, customer records, credit card numbers). Consequently, these programs serve a vital purpose in business today.

Unfortunately, many attempts are fraught with problems that result in less than satisfactory results. For many, the investment in compliance has not been adequately offset by effective risk management or measurable cost reduction. Treating compliance and related efforts as projects rather than sustainable programs and capabilities is often the culprit. At other times, labor-intensive practices that strain already burdened staff are to blame.

This whitepaper describes an effective approach for IT compliance – NetIQ's compliance and risk management methodology – and how to leverage NetIQ's methodology and solutions to consistently achieve better results.

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.

**© 1995-2007 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 Based Service Assurance, 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.

---

# Mandates for IT Compliance and Risk Management

The mandates for compliance come from many sources. Perhaps the most common source is the information security policies of the organization. Unfortunately, many organizations do not have robust or complete information security policies, and leave the decision-making for security implementation up to the technologist rather than the management of the company. One of the auditor's first procedures should be the evaluation of information security policies, to see if they exist and to assess them for appropriateness. From there, the auditor should evaluate the configuration and other security aspects of key systems and the network with policies for guidance. However, given that policies are often limited, the auditor should go beyond policies during the audit in order to identify other causes of risk.

Compliance, too, is driven by regulations and industry standards, from those that are general (e.g., Sarbanes-Oxley, Basel II Accord) to those that are more specific (e.g., HIPAA, Payment Card Industry Data Security Standard). Moreover, external auditors routinely review their clients' compliance programs as part of the financial audit.

## What Is Compliance?

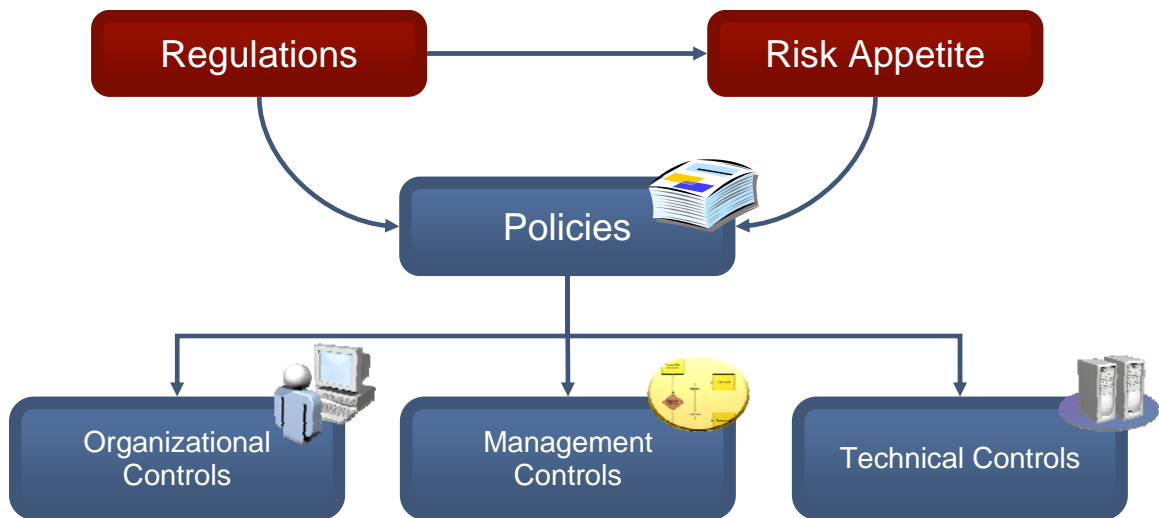
Compliance begins with executive management and the board of directors (or similar entity). At those highest levels management sets the organization's risk appetite, whether formally or informally. Risk appetite is defined in COSO's Enterprise Risk Management Integrated Framework (COSO ERM) as:

*...the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style.<sup>1</sup>*

In practice, the risk appetite of an organization is highly dependent on the nature of its business, its industry, its regulatory oversight and other factors that are outside of management's control. For example, financial services entities are entrusted with its customer's money and financial information and are bound to operate with a lower risk appetite than some other entities. Regardless, the risk appetite should be reflected in the organization's policies (and overall policy framework, including principles, standards, guidelines, etc.). In turn, policies should define the organization's control structure, as depicted below.

---

<sup>1</sup> Steinberg, Richard M. et al. Enterprise Risk Management Framework – Integrated Framework. (September 2004) Committee of Sponsoring Organizations of the Treadway Commission.



Compliance thus becomes a process of ensuring the organization is implementing and maintaining effective controls that meet or exceed the requirements set forth in policy. In doing so, management helps ensure it is operating with the risk appetite of the organization.

IT security and change controls are a large part of the control structure, especially general controls (the foundation on which effective application controls can be built). These encompass all three types (organizational, management and technical) and are the focus of IT compliance programs.

In establishing IT compliance programs, many begin to measure compliance simply by whether or not the controls are properly implemented and maintained. For example, controls governing identification and authentication, such as password requirements, are assessed as part of the compliance program. Unfortunately, there are several limitations of this approach:

- ☑ Not all controls should be treated (or weighted) equally. Some control deficiencies represent a much greater risk to the organization than do others. For example, an administrator account with no password would represent a greater vulnerability on a machine than a limited privilege account with no password. In essence, this “binary” (yes or no) approach distorts the assessment of controls and often forces management (or administrators) to focus on costly controls that do not reduce a significant amount of risk.
- ☑ Not all systems should be treated (or weighted) equally. Different systems represent different values to the business. For example, the primary server supporting the organization’s ERP system (e.g., Peoplesoft) is much more vital to the business than a backup e-mail server. The assessments should consider the importance of the systems to the business so that management can focus its resources on protecting what are most critical.
- ☑ Some controls may not be practical for certain systems. Oftentimes policies dictate controls that cannot be implemented on every system without having a detrimental impact. For example, service accounts, which are used by applications or other services to start up on a machine, often require passwords that do not change. Many organizations maintain a policy – rightly so – that requires user accounts to have passwords changed every so many days. Obviously, this policy is impractical on important service accounts. Exceptions have to be made.

Risk management, when performed properly, overcomes these limitations.

## Risk Management

Risk management is often described as the next wave of IT governance. This is evident in standards and frameworks such as COSO ERM, ISACA's Control Objectives for Information and Related Technology (COBIT), ISO/IEC 17799:2005 (and equivalents) and others. These, in turn, are used to interpret regulations such as Sarbanes-Oxley (and quite likely the EU Eighth Directive<sup>2</sup>) and industry standards such as Basel II Accord.

Risk management depends on the ability to effectively measure and mitigate risk, regardless of its form or cause. In the case of IT security, risk is generally expressed as a function of threats, vulnerabilities and business impact:

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$

Unfortunately, the level of threats and business impact are very difficult to reduce. Threats are a factor of the business and technical environment, encompassing not only hackers but also automated threats like worms and viruses and rogue insiders like disgruntled employees. Business impact is merely derived from the business value of the particular technology: the destruction or compromise of a mission critical business application is going to have a much greater impact than that of a non-critical system.

As a result, the focus of risk management should be on managing the elements that can be managed. Specifically, an organization should monitor the threat environment and identify, respond to and resolve threats and incidents quickly and efficiently. Vulnerabilities should also be identified and remediated or mitigated (as appropriate) on a timely basis. Failing to manage these factors often results in a less than satisfactory, and often quite expensive, approach to IT compliance.

---

## NetIQ's Methodology for Compliance & Risk Management

NetIQ has defined a three-stage, nine-activity methodology for compliance and risk management. This methodology is largely based on principles from leading compliance and risk management frameworks such as COSO's Enterprise Risk Management Integrated Framework<sup>3</sup>, ISACA's Control Objectives for Information and Related Technology (COBIT), the National Institute of Standards and Technology (NIST) risk management framework (based on numerous Special Publications and Federal Information Processing Standards), and others. Unlike these frameworks and models, however, our methodology provides the flexibility to fit almost any process that has been implemented by a specific organization.

NetIQ's methodology is best illustrated by the following diagram:

---

<sup>2</sup> While the Directive does not require the independent assessment and reporting on the effectiveness of internal controls (as required by Sarbanes-Oxley), it will probably require companies to report any material weaknesses in internal controls (including IT general controls) for financial reporting.

<sup>3</sup> Steinberg, Richard M. et al. Enterprise Risk Management Framework – Integrated Framework. (September 2004) Committee of Sponsoring Organizations of the Treadway Commission.



**Figure 1: NetIQ's three-stage, nine-activity compliance and risk management methodology.**

There are several primary components to the methodology that are worth discussing, in addition to the stages and activities. These also include the policy framework and metrics and reporting.

## Policy Framework

The policy framework is represented by the middle of the diagram, with the words “Policies | Standards | Guidelines | SLAs | OLAs | Contracts”. This framework would include the mandatory information security policies, standards and guidelines. They might also include those measures agreed upon as part of service-level agreements as well as those negotiated with third parties, such as vendors and business partners. Think of these as the business rules for security. They can be numerous and varied.

NetIQ provides a powerful solution for developing, reviewing, approving and communicating policies, standards and other policy framework documents. NetIQ’s award-winning VigilEnt Policy Center has been deployed by hundreds of organizations to ensure their people have read and understood the policies that apply to them. In addition, these organizations leverage VigilEnt Policy Center to ensure people agree to abide by the policies, providing crucial evidence of compliance.

## Assess

*Assess: A review, inventory or audit of the environment and compliance with the business rules (e.g., SLAs, OLAs, policies, etc.).*

Assessments provide an accurate picture of the technical security posture – the *state* of IT security – at any given point. To be effective, assessments should be performed routinely, such as once a month, and be automated. Assessments are often performed by a dedicated compliance team, often within the IT security department; however, they can also be performed by auditors (internal or external) and by administrators. Since compliance requires a certain level of independence, auditors and/or a compliance team should lead the assessment process and ensure its objectivity.

As detailed below, the activities for the assessment stage are directly supported by NetIQ's Secure Configuration Manager, a policy-based enterprise-class security configuration and vulnerability management solution. This document does not fully describe NetIQ Secure Configuration Manager, its features and functions or its technical architecture. However, it does illustrate how NetIQ Secure Configuration Manager supports the NetIQ compliance and risk management methodology.

In performing assessments, you will better know what to protect and how much to spend on protection. You will also ensure protection and risk management are based on policies (business rules), rather than on the ad hoc judgment of administrators and architects. Finally, you will be able to focus your security efforts based on accurate assessments and business priorities.

The assess stage is characterized by three primary activities:

- (1) **Inventory and Prioritize Systems:** To assess and protect your environment and ensure compliance, you must know what exists and how important it is to your business. Some organizations have begun to effectively manage their IT inventory, using such practices as ITIL configuration management and a corresponding configuration management database (CMDB). Many others are not so fortunate and struggle with determining what they have in place and how important their systems are to the business.

NetIQ Secure Configuration Manager supports numerous methods of discovery, including discovery via Active Directory, DNS, NIS and other methods, as well as natively importing nmap scan results (our preferred method for scan-based discovery).

NetIQ Secure Configuration Manager also supports the prioritization of assets based on their importance to the business. These must be manually entered as part of your procedures (as they cannot be automatically discerned), but provide for truly risk-based metrics and reporting. Without importance levels, all assets would be treated the same, making it difficult to get a true picture of business risk or to prioritize efforts.

While NetIQ Secure Configuration Manager is not designed to provide a complete IT inventory management system, it often leverages existing IT inventories (by importing managed systems) and feeds into them (especially CMDBs). For example, NetIQ Secure Configuration Manager can update an inventory system with the latest configuration (e.g., service packs, hotfixes, services running, applications installed, etc.) of given assets.

- (2) **Grade Compliance to Standard Baselines:** A critical component for compliance programs is the assessment of systems against a defined set of security standards. For example, many organizations adopt benchmarks based on generally accepted practices, such as the benchmarks from the Center for Internet Security (see [www.cisecurity.org](http://www.cisecurity.org)). These benchmarks define the minimum acceptable configuration of a system for security. Many organization's also supplement their security benchmarks with operational requirements, such as services that must be running to support an application, required service accounts and minimum free disk space.

NetIQ Secure Configuration Manager allows customers to define their technical security baselines for critical platforms such as Windows, UNIX, Linux, and iSeries (AS/400). It then automates the routine assessment of critical servers and workstations according to those baselines (policies) and scores policy exceptions according to pre-defined or customer defined settings. By combining the scores with the asset importance levels, NetIQ Secure Configuration Manager provides risk-based compliance metrics.

- (3) **Identify Vulnerable & Exploited Systems:** Another critical component is the identification of systems with vulnerabilities and those that have been exploited (e.g., compromised or infected). Policies usually mandate protection against known vulnerabilities and threats. Vulnerabilities can be defined as:

*A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an organization's operations or assets through a loss of confidentiality, integrity, or availability<sup>4</sup>.*

Vulnerabilities generally stem from configuration flaws, missing patches, running dangerous or unnecessary services, and having exposed (poorly protected) user accounts or default accounts. Consequently, any solution for identifying vulnerable systems must address all of these sources.

While typically purchased and implemented for assessing technical compliance, NetIQ Secure Configuration Manager provides robust vulnerability assessment as well. It goes beyond traditional network vulnerability assessment products by providing exceptionally accurate identification of vulnerabilities as well as the identification of already exploited systems.

In essence, it identifies vulnerabilities and exploits using the same methods an administrator would use if he or she wanted to see if a system was vulnerable or compromised, such as by looking at files, registry keys, patch levels and so forth. Network vulnerability assessment tools, while cheap and easy to deploy, miss many vulnerabilities and create false positives because they scan ports, looking for tell-tale signatures. In contrast, the method used by NetIQ Secure Configuration Manager is highly accurate and scalable and does not flood the network with malformed packets and other noise.

NetIQ has also partnered with leaders in the security research space – MITRE<sup>5</sup> and Cisco Security Intelligence Service. These partnerships provide users of NetIQ Secure Configuration Manager with security checks and bulletins for the latest vulnerabilities and threats, such as worms and viruses. What's more, we provide the automated checks for these issues, giving customers the most up-to-date checks for vulnerabilities and exploits.

---

<sup>4</sup> Source: NIST Special Publication 800-53: [Recommended Security Controls for Federal Information Systems](#) (Initial Public Draft), October 2003




<sup>5</sup> NetIQ Secure Configuration Manager supports both the Common Vulnerabilities and Exposures (CVE, <http://cve.mitre.org>) and Open Vulnerability Assessment (OVAL, <http://oval.mitre.org>) programs from MITRE.



## Worm: Zotob

**MALICIOUS CODE ALERT**

Threat Type: **Malicious Code: Worm**  
IntelliShield ID: **9591**  
Version: **2**  
First Published: **Aug 15, 2005; 11:32 AM EDT**  
Last Published: **Aug 16, 2005; 09:54 AM EDT**  
Ports: **445, 8888, 33333**  
CVE: **Not Available**

**Urgency: Possible Use**   
**Credibility: Confirmed**   
**Severity: Moderate Damage** 

**Version Summary:** **Zotob.C is a variant of Zotob.A, which allows unauthorized remote access to the infected system. The variant now contains its own mass-mailing component. Multiple vendor have released virus definitions to detect Zotob.C and Zotob.A.**

**Variants** The only known variant is **Zotob.C (F-Secure)**.

**Virus Name:** **Zotob.A** (Aliases include **Zotob.A (Aladdin)**, **Win32.Worm.Zotob.A (BitDefender)**, **Win32.Zotob.A (Computer Associates)**, **Win32.Zotob.B (Computer Associates)**, **Win32/Mytob.IQ (eSet)**, **Win32/Mytob.IR (eSet)**, **Zotob.B (F-Secure)**, **Worm.Win32.Mytob.FR (Hauri)**, **W32/Zotob.worm (McAfee)**, **W32/Zotob.worm.b (McAfee)**, **W32/Zotob.worm.gen (McAfee)**, **Zotob.A (Panda)**, **Zotob.B (Panda)**, **W32/Zotob-A (Sophos)**, **W32/Zotob-B (Sophos)**, **W32.Zotob.A (Symantec)**, **W32.Zotob.B (Symantec)**, **WORM\_ZOTOB.A (Trend)** and **WORM\_ZOTOB.B (Trend Micro)**.)

### Description

**Zotob.A** is a worm that allows unauthorized remote access to the system and propagates by exploiting the Microsoft Windows plug and play remote code execution vulnerability as described in Microsoft Security Bulletin MS05-039 and Cybertrust Alert 9572.

When executed, the worm copies itself as either **botzor.exe** or **csn.exe** to the %System% folder. The worm modifies the system registry to ensure it runs each time Windows starts and to bypass or disable various security features. The worm creates the mutex **B-O-T-Z-O-R** to ensure only one instance of the worm is running at a time.

**Figure 2: Vulnerability and exploit bulletin in NetIQ Secure Configuration Manager from Cisco (formerly TruSecure). The bulletin text contains detailed information for investigating and resolving vulnerabilities and threats. NetIQ Secure Configuration Manager also provides automated checks to determine which systems are at risk.**

## Operate

***Operate:** The daily monitoring and administration to meet the business rules (the policies), including detecting and responding to service problems, security breaches, and unauthorized or potentially damaging changes.*

The operations stage is characterized by monitoring, but also includes the practice of incident management. Security operations – when implemented most effectively – are usually integrated into the organization’s existing processes and procedures for IT operations, such as incident, problem and change management. However, care must be taken to include specific provisions for security-related incidents, which often require security-specific expertise (e.g., computer forensics) and the proper handling of evidence.

As detailed below, the activities for the operate stage are directly supported by NetIQ Security Manager, a rules-based enterprise-class security incident and event management solution. This document does not fully describe NetIQ Security Manager, its features and functions or its technical architecture. However, it does illustrate how NetIQ Security Manager supports the NetIQ compliance and risk management methodology.

Effective security operations will reduce the business impact of threats to security and performance. It does this by reducing the time for responding to and resolving security incidents and providing a more measured response. It will also help ensure all incidents are escalated and resolved according to SLAs and standard operating procedures.

The operate stage is characterized by three primary activities:

- (1) **Efficiently Review Security Logs & Events:** Many IT security-related regulations (e.g., HIPAA<sup>6</sup> Security Rule) and standards (e.g., COBIT) require system or security activity reviews. This effectively means the periodic review of logs, often a time-consuming and tedious exercise. Further complicating the matter, many organizations are mandating the consolidation and archival of log files in order to ensure they are available during reviews or investigations.

NetIQ Security Manager provides the consolidation of security and other logs from critical servers and devices, such as Windows, UNIX, Linux, and iSeries servers as well as network devices (e.g., Cisco routers and switches, Check Point firewalls), antivirus applications and more. It then enables summary reporting, online analysis (via OLAP), and robust query capabilities for the data warehouse of log files that it creates and maintains. In doing so, customers can reduce the time for reviewing log files from hours to minutes, and meet or exceed many regulatory requirements.

- (2) **Detect Threats, Changes & Policy Violations:** Threats vary from automatons (e.g., worms and viruses) to disgruntled employees to external hackers and criminal. They can be very sudden and dynamic and are impossible to predict. However, changes (especially those that are unauthorized) and policy violations can significantly compromise the security of systems, exposing them to risks or directly causing performance problems.

NetIQ Security Manager also provides the automated detection of security events and incidents, such as potential intrusions, system changes, and policy violations. It does this by providing host-based IDS on Windows, UNIX, Linux and iSeries, as well as integrating, filtering, correlating and alerting on third-party events (e.g., network IDS, intrusion prevention, firewalls, and antivirus).

- (3) **Manage Security Incidents:** As threats vary so do incidents. Security incidents include attacks (both attempted to successful), policy violations such as unauthorized access of resources, and changes (authorized or not) to security and control mechanisms. The nature of the incident dictates the procedures for, speed of and personnel involved in the response. Moreover, some security incidents do not require a response, but should be recorded for metrics-based reporting and potential future investigations.

NetIQ Security Manager supports rapid incident response and tracks security alerts through resolution. For example, NetIQ Security Manager improves response and resolution times by making security logs accessible and easily queried. With NetIQ Security Manager, incident response teams have log information at their fingertips. NetIQ Security Manager also tracks security events and alerts through response steps, such as acknowledgement, first-level assignment and so forth. Deviations from agreed-upon response times are also tracked.

---

<sup>6</sup> Health Insurance Portability and Accountability Act, as embodied in 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule.

**Forensic Analysis Report**  
Dave Burgess Search  
Created on SERVER01

Network Node Address: 10.21.16.91

Event Instance Id	Network Node Name	Event Timestamp (UTC)	Source Name	Severity	Source Address	Source User	Source Protocol	Source Port
Network Node Address: 10.21.71.157								
Native Classification: 612								
Native Classification: 593								
71346	Demo_Win1	2/16/2004 10:57:34 AM	Security	low	10.21.71.157	mle		
71320	Demo_Win1	2/16/2004 10:58:18 AM	Security	low	10.21.71.157	mle		
71315	Demo_Win1	2/16/2004 10:58:23 AM	Security	low	10.21.71.157	mle		
Native Classification: 592								
Native Classification: 578								
71335	Demo_Win1	2/16/2004 10:57:38 AM	Security	low	10.21.71.157	mle		
71330	Demo_Win1	2/16/2004 10:58:02 AM	Security	low	10.21.71.157	mle		
71325	Demo_Win1	2/16/2004 10:58:16 AM	Security	low	10.21.71.157	mle		
Network Node Address: 10.21.76.120								
Native Classification: WEB-IS unicode directory traversal attempt								
Native Classification: WEB-IS perl-access								
Native Classification: WEB-IS rootadmin access								
200168	Demo_Snort1	2/15/2004 5:17:10 AM	sid	low	4.4.4.4			32829
200210	Demo_Snort1	2/15/2004 6:36:28 AM	sid	medium	1.1.1.1			32829
200228	Demo_Snort1	2/15/2004 7:10:27 AM	sid	medium	3.3.3.3			32829
200300	Demo_Snort1	2/15/2004 9:26:23 AM	sid	medium	1.1.1.1			32829
200318	Demo_Snort1	2/15/2004 10:00:22 AM	sid	medium	3.3.3.3			32829
200348	Demo_Snort1	2/15/2004 10:57:00 AM	sid	low	4.4.4.4			32829
200390	Demo_Snort1	2/15/2004 12:18:18 PM	sid	medium	1.1.1.1			32829
200408	Demo_Snort1	2/15/2004 12:50:17 PM	sid	medium	3.3.3.3			32829
200480	Demo_Snort1	2/15/2004 3:06:13 PM	sid	medium	1.1.1.1			32829
200498	Demo_Snort1	2/15/2004 3:40:12 PM	sid	medium	3.3.3.3			32829

**Figure 3:** Results of a forensic query of NetIQ Security Manager’s consolidated log files. Query results are returned in an easy-to-navigate data analysis window.

NetIQ Secure Configuration Manager also supports incident response by providing configuration data to the response team. It makes it easy to compare the configuration of critical servers and workstations at one point in time (say, after a breach) to another (say, the last known good image). This delta reporting is highly effective during incident investigation.

**Vulnerability Manager Delta Report Viewer**

Delta Report for Policy Template 'CIS Level One Benchmark for Windows 2000' (creation time: 2/14/2005 1:33:13 AM)

This report shows the result of delta comparison of the policy template 'CIS Level One Benchmark for Windows 2000' run at '2/14/2005 1:32:54 AM' to the base policy template 'CIS Level One Benchmark for Windows 2000' run at '2/13/2005 6:56:05 PM'

Delta Comparison View | Full Report

**Security Checks**  
43 Records

Check Name	Platform	Endpoint Name	Delta	2/13/2005 6:56:05 PM	2/14/2005 1:33:13 AM
Delta: Modified					
Account lockout duration	Windows Common	agility	Modified	System	System
Account lockout reset time	Windows Common	agility	Modified	System	System
Account lockout threshold	Windows Common	agility	Modified	System	System
Delta: Unchanged					
Account logon events failure auditing	Windows Machine	agility	Unchanged	Audit/Auth Analysis	Audit/Auth Analysis

**Figure 4:** NetIQ Secure Configuration Manager’s delta reports quickly highlight changes that have been made since a previous assessment, facilitating investigations.

## Control

*Control: The creation of preventive or corrective controls to mitigate risks of compliance exceptions or breaches of confidentiality, integrity and availability.*

Effective controls are the objective of the policy framework. They are the mechanisms that ensure compliance with mandates and regulations as well as mitigate or manage the risks associated with information and related technologies. The control stage seeks to implement preventive controls where possible, as dictated by policies and other guidance, or corrective controls. It is the natural result of both the assessment stage, which identifies control weaknesses, and the operate stage, which detects changes to controls and breaches of controls.

The control stage must be flexible. While implementing controls based strictly on policies and standards is desirable, it is often not possible. Consider the example of service accounts described above (they often cannot have their passwords changed). In those cases where policy-mandated controls cannot be enforced, mitigating or compensating controls must be considered. Our methodology includes this consideration and our solutions support the implementation of compensating controls.

The activities for the control stage are directly supported by NetIQ's VigilEnt Policy Center, Secure Configuration Manager and Security Manager. However, other solutions may also be used to support the implementation of controls. For example, NetIQ's Security Administration Suite may be used to implement configuration standards on Windows platforms by leveraging the power of Microsoft group policy. This document does not fully describe NetIQ's solutions but it does illustrate how they support the NetIQ compliance and risk management methodology.

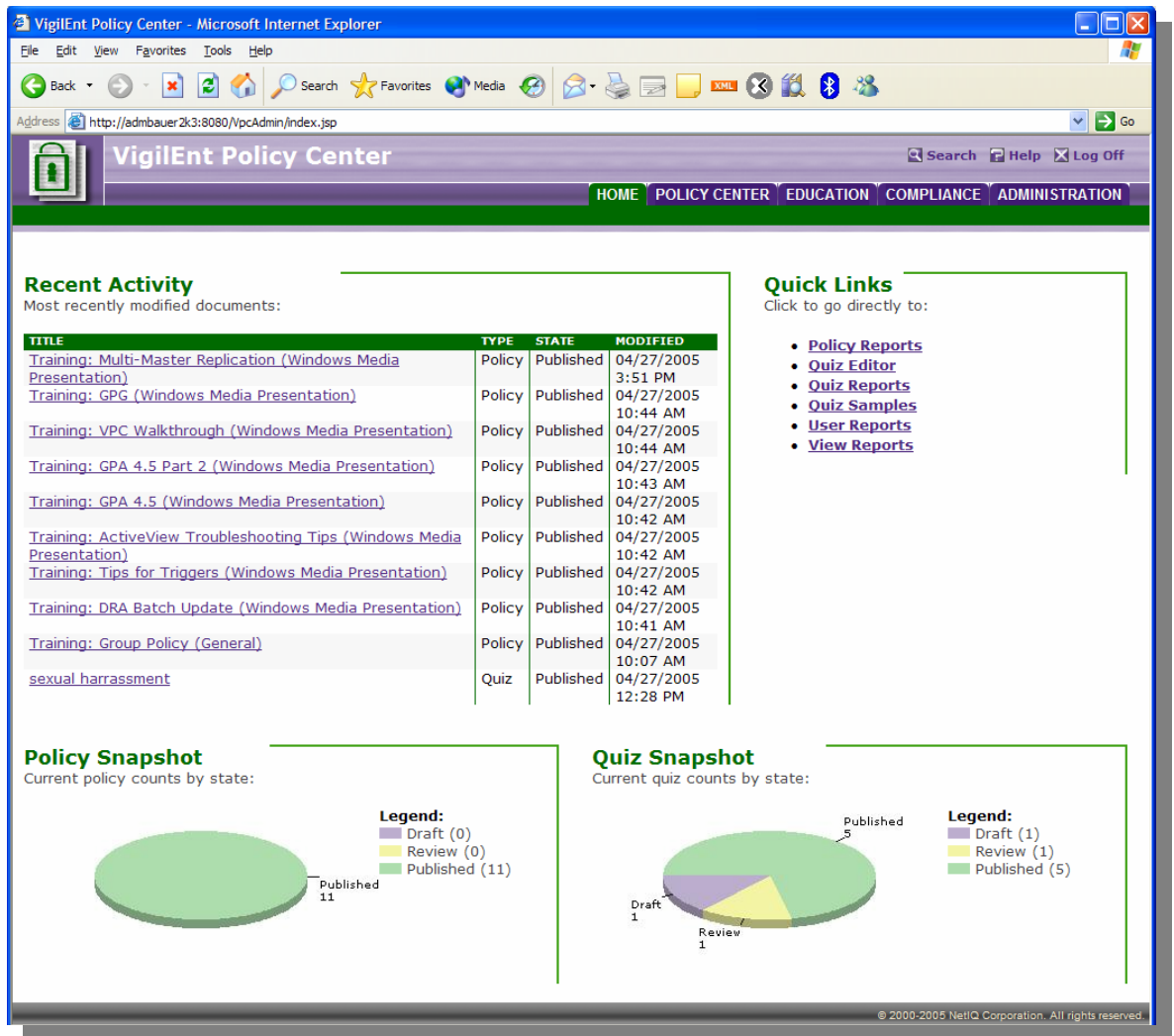
By properly and methodically addressing controls, you will establish a security posture that is in line with your organization's risk appetite. It will be defensible to your auditors, even though policy exceptions may exist. You will also benefit from bolstering your first line of defense – your people – while reducing the cost of security management through standardization. Finally, you will often be able to mitigate risk without requiring significant changes or interruptions to production.

The control stage is characterized by three primary activities:

- (1) **Educate Employees & Improve Awareness:** Employees and other workers in your organization can be a significant source of security incidents. Many times these are not the result of malice on their part, but rather ignorance. Consider the number of incidents caused by Trojan horse programs; these take advantage of naïve PC users, not always unprotected PCs.

However, the bigger concern relates to uninformed administrators, architects and other technical personnel directly responsible for designing and implementing security controls. Many organizations fail to ensure these vital personnel are knowledgeable of adopted security standards. For example, many corporate Windows administrators do not know how to properly secure a Windows server!

NetIQ's VigilEnt Policy Center helps solve this problem. VigilEnt Policy Center provides role-based distribution of policies, standards and other documents. For example, VigilEnt Policy Center can distribute Windows hardening standards to all Windows administrators, based on their membership in specified containers in Active Directory. It can also require those administrators to digitally sign the document, agreeing to abide by (or enforce) the standards. Exception reports help compliance managers target areas of need, enabling them to cost-effectively improve awareness. Moreover, quizzes can be administered to gauge understanding and awareness.



**Figure 5: VigilEnt Policy Center enables policy authors to manage content such as policy documents and quizzes. Administrators can also set up users and roles by leveraging an existing directory (e.g., Active Directory) and publish content to employees based on their role.**

- (2) **Enforce Configuration Standards:** Security configuration standards help establish a known risk and security posture of an asset. The assess stage often identifies exceptions to the configuration standards when grading compliance to baseline standards. Moreover, the operate stage often identifies (often in real-time) changes to system configurations that bring a system out of compliance. Enforcing those standards is often the preferred method of dealing with those issues or incidents.

NetIQ Secure Configuration Manager provides the information to know exactly where and how to remediate compliance exceptions and vulnerabilities. Specifically, it provides detailed reports on exceptions, such as which accounts violate a given policy check or which patches have not been applied. It also provides instructions for remediation, often including highly detailed instructions from TruSecure.

NetIQ Secure Configuration Manager also feeds assessment results into existing processes and tools for remediation via operations staff. Specifically, NetIQ Secure Configuration Manager feeds compliance exceptions and vulnerabilities to NetIQ Security Manager via out-of-the-box integration. In turn, those results can be fed into NetIQ AppManager for the IT operations. Furthermore, NetIQ Secure Configuration Manager feeds trouble ticketing systems via a configurable API.

Finally, NetIQ provides remediation capabilities for Windows platforms through its Security Administration Suite. Security Administration Suite provides extensive administration capabilities for Windows and Active Directory. It also helps organizations safely leverage Microsoft group policy, which in turn can implement many configuration standards.

- (3) **Implement Compensating Controls:** Since systems oftentimes cannot be brought into compliance, it is important to be able to implement compensating controls to address the risk. The example used above is service accounts used by applications. These often have significant privileges (especially for data access) and yet cannot be protected by changing their passwords on a frequent interval (doing so breaks the application). Organizations in this situation should seek a compensating control to mitigate (or minimize) the risk associated with the service accounts.

NetIQ supports compensating controls. In the service account example used above, NetIQ Security Manager can be used to monitor the service account for changes, interactive logins, and other suspicious or unusual activities. NetIQ Secure Configuration Manager can routinely assess the service accounts for the *ability to* login interactively, for the strength of their existing passwords, for other privileges and so on. In doing so, organizations can properly address the risks presented by service accounts when they cannot be brought into compliance.

Another common example relates to change controls. Control weaknesses often result when IT managers grant employees powerful (and permanent) privileges to production servers in order to accomplish narrow tasks that need to be done only infrequently. This situation exists because native permissions fail to offer the kind of granularity that today's regulatory environment requires. NetIQ Change Administrator addresses this problem. With NetIQ Change Administrator, change implementers access servers through a controlled interface, which mediates access to the server, limiting the user to specified applications or commands during a specified period of time.

There are many other examples of how NetIQ solutions can help implement or enforce compensating controls. Ultimately, compensating controls must be chosen by management according to a defined process that considers the nature of the policy exception.

## Metrics and Reporting

In order to achieve continuous improvement – an objective of most compliance and risk management programs – organizations must be able to measure progress. Metrics come in many varieties, but ultimately must illustrate compliance to regulatory requirements and other business drivers as well as demonstrate managed risk.

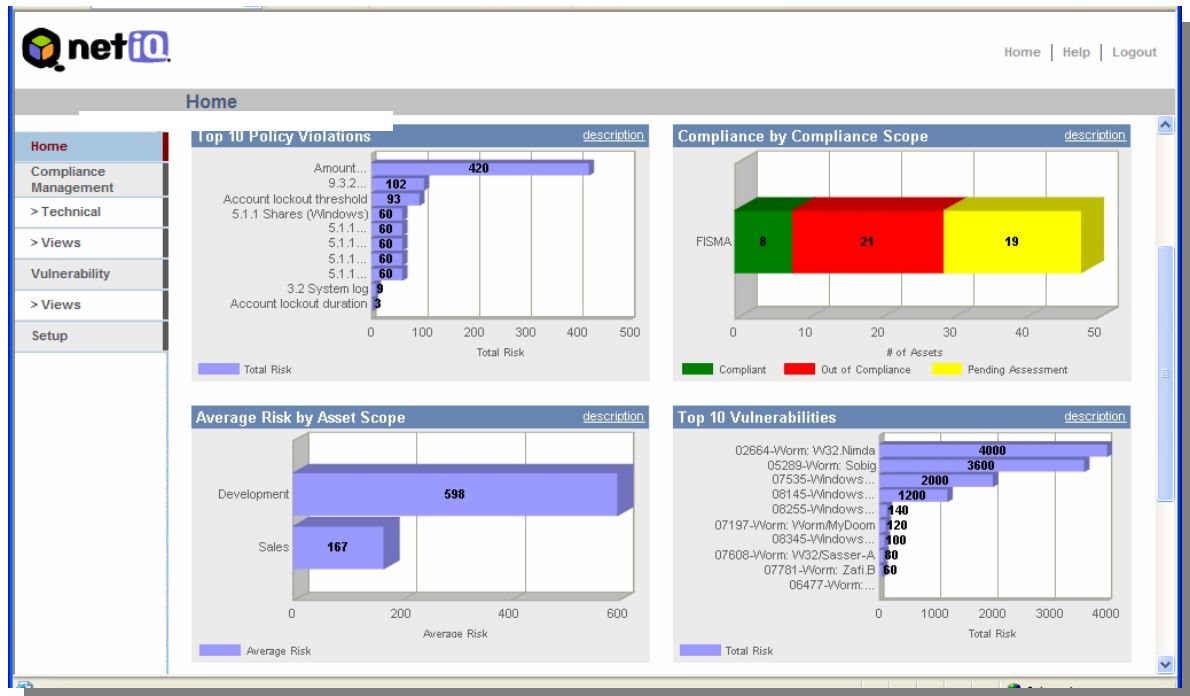
Most organizations begin with simple, easily provable metrics for security. Examples of such metrics are listed below, along with other types of reports that are common in mature compliance and risk management programs.



While such product-specific reports are powerful, they are only useful if they are communicated to the appropriate stakeholders. Moreover, most are only useful when put into the context of the compliance drivers, such as regulations or standards. This is where NetIQ's Risk & Compliance Center comes in.

## Pulling It All Together – NetIQ Risk & Compliance Center

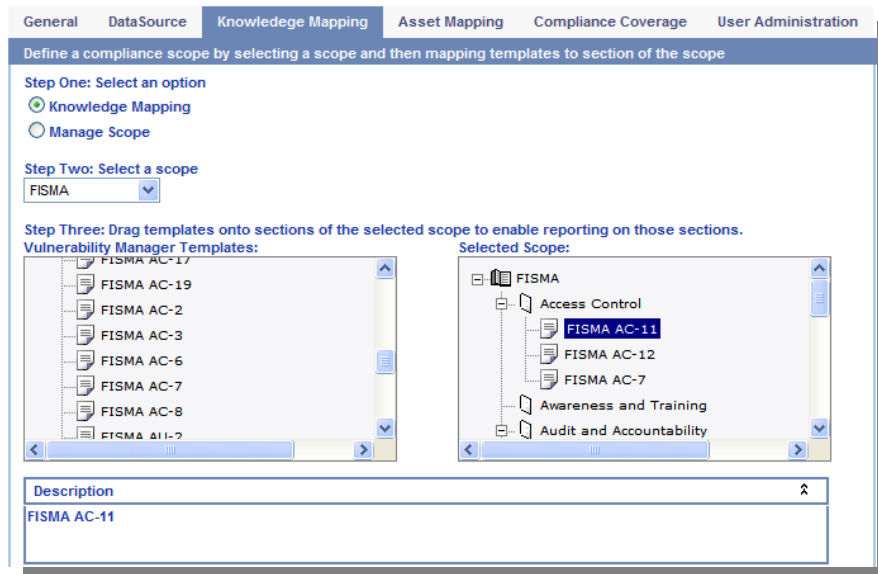
NetIQ Risk & Compliance Center is a forthcoming<sup>7</sup> dashboard for executive and managerial compliance and risk management. Risk & Compliance Center communicates compliance and risk metrics to executives and managers through a web-based portal. It enables users to access and analyze the metrics provided by the underlying compliance and risk management products (e.g., NetIQ Secure Configuration Manager).



**Figure 6: Risk & Compliance Center's main page can be tailored to illustrate different aspects of compliance and risk management.**

Risk & Compliance Center helps illustrate compliance to specific business drivers by enabling customers to map (link) them to specific metrics from the underlying products. For example, Risk & Compliance Center enables US federal customers to link compliance checks in NetIQ Secure Configuration Manager to specific sections of NIST Special Publish 800-53.

<sup>7</sup> The first release of Risk & Compliance Center is scheduled for release in late calendar 2005. It will integrate with NetIQ Secure Configuration Manager. Releases in early to mid-2006 will integrate with VigilEnt Policy Center and NetIQ Security Manager.



**Figure 7: NetIQ Risk & Compliance Center allows underlying Secure Configuration Manager templates to be mapped to specific regulations or standards, which later provide a distinct view of compliance.**

While Risk & Compliance Center will initially leverage data from NetIQ Secure Configuration Manager, it will later consume and present data from VigilEnt Policy Center and NetIQ Security Manager in order to illustrate compliance and risk beyond the technical configuration of technologies. For example, it will present metrics on security awareness, intrusions, policy violations and other indicators of compliance and risk.

---

## About NetIQ Corporation

### *A World Leader in Systems and Security Management*

NetIQ delivers business-critical solutions to assure, analyze and optimize the performance, availability and security of your IT infrastructure.

Only NetIQ supplies the best-of-breed tools you need to Work Smarter—to manage and secure your critical infrastructure investments, such as servers, databases, web sites, email, voice and video and mission-critical applications. Not only can we help you customize and refine your Systems Management and Security Management controls to fit your particular environment, but we can also provide critical insights into your web site performance.

Focused on providing you with the competitive advantage necessary to survive and thrive in today's chaotic business environment, NetIQ offers a complete range of easy-to-deploy, cross-platform solutions—from our industry- and market-leading Windows Systems Management solutions to our solutions for Linux and UNIX; and from our integrated Security Management products to our award-winning WebTrends Web Analytics tools.

NetIQ counts more than 4,000 of the world's leading enterprises as key customers. In addition, our partnerships with industry leaders, such as Microsoft, IBM, HP and Dell, give NetIQ a unique advantage in the global marketplace. With customer-proven solutions and strong relationships, NetIQ delivers the tools you need to reduce your risk and deliver value from day one.

To learn more about NetIQ, visit us online at [www.NetIQ.com](http://www.NetIQ.com).