



Contents

Financial Services Industry Overview	1
Regulations Impacting Financial Services.....	5
Other Laws and Standards Affecting Financial Services.....	9
NetIQ Security Solutions	10
Achieving Compliance with NetIQ	16
About NetIQ Corporation	19

Assuring Compliance for Financial Services

January 2006

As a financial services provider, you are faced with growing government regulations, an increasing number of audits and ever evolving threats. There is tremendous pressure to maintain data in a secure and accountable fashion and mitigate risks to your information systems.

Regulations and audits are a way of life for security officers in the financial services industry. For example, the Gramm-Leach-Bliley Act (GLBA) requires banks and financial institutions to implement comprehensive written information security policies to safeguard customer data. Likewise, the Sarbanes-Oxley Act of 2002 requires all publicly held companies to establish and maintain internal controls over their financial reporting systems and ensure their effectiveness.

The cost of noncompliance with regulations can run high—prison terms, monetary fines and loss of company reputation. This reality has fueled the growth of companies in establishing and adhering to IT security programs for assuring compliance.

The bottom line is that security management is a major business issue for financial services. Complete security management includes assuring compliance, managing risks and securing assets. Security helps ensure trust, and financial services are founded on trust—of customers, business partners and the government. But can you ensure trust if you haven't defined, communicated and implemented a comprehensive security policy? How can you earn trust if you cannot demonstrate compliance and security?

This guide describes many of the challenges financial services institutions face in the area of regulatory compliance. It also describes the comprehensive solutions that NetIQ provides for addressing these key challenges.

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.

Financial Services Industry Overview

The Financial Services Industry is actually composed of several sub-segments. There are three main sub-segments in this industry: banking, securities and insurance. Each of these sub-segments is further divided down into the categories below.

The banking sub-segment includes:

- Federal Reserve Banks
- Commercial Banks
- Savings Institutions
- Credit Unions
- Federal, Personal and Business Credit Organizations
- Mortgage Brokers

The securities sub-segment includes:

- Securities Brokers
- Commodities Brokers
- Exchanges
- Investment Services

The insurance sub-segment includes:

- Life Insurance
- Property and Casualty Insurance
- Pension Funds
- Insurance Agents and Brokers

These three sub-segments were formed as a result of the changes in the U.S. financial system in the 1930s. The Great Depression led to a crisis in the banking system, as almost one quarter of all national banks failed. This was believed to be partly the result of the environment where banks routinely were the underwriters of insurance policies purchased by their customers, as well as managing their customers' brokerage activities. Therefore, the Banking Act of 1933, also known as the Glass-Steagall Act, forced banks, insurance companies and brokerages to operate as separate entities with regulated methods for interaction.

The three sub-segments within the financial services industry each have had a specific focus on products and services that they deliver to customers. Traditionally, banking institutions provide direct deposit accounts, such as checking and savings accounts, along with providing loans for customer purchases of large-ticket items as houses, automobiles and boats. Profits are derived from the differences in interest rates; the rates the banks are charged to borrow money versus the rates they charge to lend it. Securities organizations provide customers with the opportunity to purchase stocks and bonds, and also provide financial planning advice in the areas of investments and retirement planning. Brokers make money on the commissions that they charge, frequently on a per-transaction (either buy or sell) basis.

Insurance products are purchased to protect against loss due to personal injury, health decline, property damage or loss and the liability due to negligence. Policies are sold to individual consumers or corporations for a price, which is based on an initial assessment of the expenses to maintain the policy. Pricing is based upon the value of the item insured.

Key Business Trends in Financial Services

Several key trends have emerged over the past few years in this industry. Across all of these, a key enabler is technology. Where technology was once used only as an implementation tool for business strategies, now it is integrated much earlier into the decision process, as a factor in choosing which strategies to pursue. At the beginning of the 21st century, the financial services industry accounted for over 15% of the total global IT purchases.

Convergence is the leading trend in financial services. This means that the barriers separating banks, brokerages and insurers are coming down. The Gramm-Leach-Bliley Act makes it easier for entities in the three major sub-segments to sell products from the others. This trend in the U.S. is in keeping with the convergence that has already begun throughout Europe, where large institutions such as Deutsche Bank offer multiple financial products to their customers. In particular, banks are taking the lead by offering more insurance products. While the share of total consumer assets owned by banks has declined from 35% in the 1970s to less than 25% today, the share owned by mutual funds has increased from less than 10% to almost 50%. In addition, today over one third of all U.S. banks sell some form of insurance, the most common being term insurance tied to other transactions.

Consolidation within each of the three major sub-segments is also occurring. Financial institutions are drawn to acquisitions as a way to achieve economies of scale and reduce operating expenses and increase market share. The number of banks in the U.S. has been declining for well over a decade. In 1985, there were approximately 13,500 banks in the U.S., and this is expected to shrink to fewer than 5,000 by 2006. If, as expected, further regulatory acts continue to blur the distinction between the sub-segments, larger financial institutions will be organized as bank holding companies with several subsidiaries providing a full range of banking, insurance and securities offerings. This consolidation allows companies to diversify their product lines and also to function as true financial advisors—prime criteria that consumers have in determining which provider to select.

Changing business models for financial services organizations affects the ways these companies look to make profits. As previously mentioned, the role of technology has shifted from an application-centric focus to the formulation of business strategy. Initial enterprise strategy is now being made in the context of available technologies, making possible the co-development of processes, priorities and technologies. These technological advancements (on-line banking/trading, loan/policy processing, ATM/kiosk) serve to ease the production and distribution of financial products. As a result, customers have access to a more diverse product set and these products themselves are becoming more commoditized. The challenge for financial enterprises is to customize, and even personalize, their product lines as a primary sales strategy. Central to this theme is the change in the way some institutions are structuring their revenue models. In the past, they generated revenue on margin and were judged by potential customers on their stability. Today, this is changing to a revenue model that is based upon transactional fees. Instead of rate differences, flat fees assessed on a per usage (transaction) basis drive revenues.

Companies operating within the financial services industry are subject to a variety of **regulations** designed to assist the consumer and ensure a level playing field for participants. These regulations commonly originate from the federal government, but in the case of insurance providers, individual states also govern their activities. To do business in any state, an insurance company must be certified by that state's insurance commission—and the insurance commission of each individual state regulates the business activities of insurance companies operating within its boundaries. Future sections of this guide explore the key regulations affecting the financial services industry in more detail.

Financial services firms are subject to regular **audits** of different origins. Most companies of any size have an internal audit group. There are also audits that are performed via external sources, usually the large public accounting firms. Finally, the federal agencies or state commissions that regulate these companies also perform audits. Audits are usually performed on an annual basis, but sometimes extend to every 18–24 months. Audits cover business items, such as amount of working capital, and IT issues, including security.

The number of **electronic commerce initiatives** is on the rise, particularly in the banking sub-segment of the financial services industry. Consumers have demonstrated their preferences for on-line banking via personal computers and modems, and they are also using the telephone to transact business and to obtain account balances and information.

In addition, delivery channels to consumers are changing. Self-service channels, like the call/contact center and the Internet, have flourished, changing the way that consumers interact with the provider and driving down costs. Along the way, the functionality of the call/contact center has evolved to encompass multiple types of media.

Selling through **partnerships** with an established provider has become the most prevalent method for companies to enter new markets, particularly banks entering the insurance market. Banks that sell insurance most often do so through partnerships with established insurance providers. Because the insurance provider ultimately owns the policy and the customer, banks are able to increase revenues without having to deal with claims processing and policy maintenance.

Key IT Trends in Financial Services

Consumers are already demonstrating their ability to take advantage of technology by their growing **reliance on the Internet** for the delivery of financial products services and support. Gains of over a quarter of a billion users in 18-month periods illustrates the dynamic impact the Internet is destined to have on financial services providers' strategic directives, business models, business processes, infrastructure and investment initiatives. In capitalizing on this trend, providers need not limit their Internet strategies to simply providing a transaction-capable web site.

The Internet is changing the insurance provider market because it can supports the new business models while at the same time increasing business efficiency. This results in three key models for the insurance sub-segment:

- **Brick and Mortar** – Typical insurance providers that have a strong physical presence in the real world but lack the Internet presence required for the newer models
- **Pure Play Internet** – Organizations that have adopted a strictly Internet-only business model with little or no presence in the real world
- **Hybrids** – Providers that possess an adequate physical presence as well as an Internet basis for their business operations.

The Internet has also changed the distribution channel make-up in the insurance business. Whereas insurance traditionally has been distributed via agents, brokers or direct sales, new intermediaries are now supported. These intermediaries include aggregators (comparison shopping sites), integrators (banks or brokerages selling insurance along with their own lines) and partner web sites outside of the financial services industry (auto dealers).

In a recent IDC study on technology adoption trends in the financial sector, 30% of financial services companies reported that a **major security breach** at their company has had an extremely high impact on the deployment of security measures. In fact, out of 10 drivers, security breaches ranked second only to increased Internet usage as a key factor in security deployment. This study found that insurance companies are the most influenced by security breaches, with 32% citing an extremely high impact on deployment of security and another 12% rating it a high impact.

With the changing business models in the financial services industry, along with the trends toward strategic partnerships, more information is being shared across businesses. In the IDC study mentioned previously, **partnernets and extranets** were rated highly in terms of their impact on security deployment by nearly 20% of financial sector companies. Of the three industry sub-segments, banking rated the highest, with 30% of respondents giving this factor a high impact rating.

Another key IT trend impacting financial services providers is **mobile computing**. As consumers continue to interact with financial services providers on their own terms, the types of devices used to facilitate communications will continue to expand. Devices include desktop and laptop PCs, pocket PCs, PDAs and intelligent cell phones. The long-term viability of any particular device is dependent upon the invisibility of the technology. For a delivery method to enjoy widespread acceptance, consumers must identify with the benefits, not just the technology. For this reason, wireless phones will continue to be an important delivery medium, while video kiosks will not.

Like most industries, financial services will be affected by a **shortage of IT professionals**. This shortage is likely to be further driven by a sharp increase in demand for technology-enabled applications and by a continuing decline in the number of students majoring in computer science while in college. The Gartner Group forecasts that this shortage will continue well into 2006 and will drive IT costs upward as shortages in supply increase compensation and the use of external service providers.

One of the greatest challenges that will continue to confront banks, insurers and brokerages as their sales efforts cross segment boundaries is determining how the information systems of the separate business units will be integrated. As financial services providers struggle to adapt to a changing environment and the growing power of consumer demands, the skills required to implement the necessary technologies will be in short supply.

Regulations Impacting Financial Services

Information security, as demonstrated by the ability to holistically manage the confidentiality, integrity and availability of sensitive customer data, is an essential business requirement for all financial institutions. This is of such importance that governments have established legal and regulatory requirements related to information security and internal controls. Each of these requirements necessitates a comprehensive awareness of system and network activity to ensure that access to sensitive information is appropriate and unauthorized activities are identified and addressed. The result of non-compliance with these regulatory requirements can include serious consequences such as:

- Enforcement actions, including individual prison sentences
- Monetary fines, which could escalate well into six figures
- Loss of company reputation, should non-compliance become public

Effective compliance efforts will have the added benefit of helping to prevent the success of legal actions resulting from a security incident involving privacy, security or internal controls. Class action suits have been filed by consumers whose personal information was inappropriately disclosed. Monetary awards in the multi-million dollar range are being sought based upon the potential for identity theft and related damages. By demonstrating due care and regulatory compliance in their security and control practices, proactive financial institutions can minimize the risk of similar situations.

Regardless of the regulation, compliance requirements share a common pattern whereby the financial institution must minimally establish:

- Formal policies and procedures
- Processes to test, evaluate and maintain appropriate internal controls
- Monitoring and reporting capabilities

Depending upon the type of financial institution, there are eight regulatory agencies in the United States who are responsible for enforcement of regulations. These federal regulators perform regular examinations, usually on an annual basis. Regulatory exams evaluate the institution's overall condition, risk management and compliance with laws, regulations and sound practices. In addition to performing assessments of business practices, exams include a focus on audit practices, management oversight, systems development and acquisition and support and delivery systems for IT. These examinations yield a formal report of findings including the institution's total and component ratings. The agencies and the institutions they regulate are found in the table below.

<i>Regulatory Agency</i>	<i>Type of Financial Institution</i>
Board of Governors of the Federal Reserve System	Bank holding companies, members of the Federal Reserve System
Commodity Futures Trading Commission	Commodities brokers
Department of the Treasury, Office of the Comptroller of the Currency (OCC)	National banks, U.S branches of foreign banks
Department of the Treasury, Office of Thrift Supervision (OTS)	Savings associations insured by the FDIC
Federal Deposit Insurance Corporation (FDIC)	Banks they insure, not including Federal Reserve System members
Securities and Exchange Commission (SEC)	Securities brokers and dealers, investment companies
National Credit Union Administration (NCUA)	Federally insured credit unions
Federal Trade Commission (FTC)	Institutions not covered by the other agencies

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was signed into law on November 12, 1999 and it requires financial institutions to insure the security and confidentiality of customer records and information. The GLBA is subdivided into seven titles, many of which have significant impact on the future direction of the financial services industry in the United States.

From the time of the Great Depression in the 1930s, legislation has been in place to limit the interaction and cross product selling by banks, securities firms and insurance companies. The GLBA eliminates many of these barriers to affiliation between these institutions. It also contains important provisions for consumer protection and privacy.

Three very important areas of concern (modernization, privacy and security) to the financial services industry reside within the GLBA titles. In Title I, the GLBA establishes a framework where closer ties can exist between banks, securities firms, insurance companies and other financial services providers. In this framework, there is room for the creation of bank holding companies and financial subsidiaries for the purpose of multiple product-line selling. Previously, banks were limited to selling demand-deposit accounts; now, GLBA allows them to also sell investments, such as securities and commodities. Similarly, it allows investment brokerages to offer insurance products to their customer base.

Title V is a very significant part of the GLBA because it deals with the privacy and security of consumer information. Its purpose is to ensure that financial services providers respect the privacy of individual consumers. Corporate customer privacy issues are not addressed by the GLBA, and the legislation represents more of a minimum acceptable guideline than an industry standard or specification.

In May 2000, an interagency task force consisting of many GLBA governing agencies published Regulation P, which further defines the uses of personal consumer information by financial services providers. Under this regulation, providers must:

- Make consumers aware of their policies for safeguarding customer information prior to any purchases, including what non-public information is collected, under what circumstances it will be disclosed, and to whom it will be disclosed
- Make efforts to clearly disclose privacy policies and ensure that customers receive these disclosures on an annual basis
- Provide consumers with an easy way at any time to “opt out” of having any of their non-public information shared with other third parties

The other key part of Title V deals with security protection for consumer information. This is perhaps the most significant development of GLBA for IT personnel. While privacy can be primarily managed with policies dictating the actions of the financial institution, security must be addressed both from inside and outside the organization, using a combination of policies and tools to establish and enforce those policies. One set of guidelines under GLBA requires that providers protect customer information against threats to security, confidentiality and integrity. This information must be guarded against unauthorized access, the result of which could be harm, at worst, or inconvenience, at best, for customers. Providers must establish customer information security programs to safeguard this information.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 was enacted primarily to address corporate governance, financial reporting and internal control issues. It came about due in large part to well publicized accounting scandals at Enron and WorldCom. It applies to all U.S. publicly traded companies, not just those in the financial services industry. The deadline for compliance is staggered, with the first currently scheduled for November 15, 2004. This “first wave” includes public companies with a market capitalization of \$75 million or greater, and they must comply with Section 404 of the Act.

Section 404 required the SEC to prescribe rules mandating each annual report filed contain an internal control statement. The statement must attest to management’s responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It must also contain an assessment of the effectiveness of existing controls and procedures. The SEC’s rules, which implement the internal control requirements of the act, were published in June 2003 under the title “Management’s Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.”

The outlined requirements for control over financial reporting include:

- A statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting for the registrant.
- A statement identifying the framework used by management to evaluate the effectiveness of the registrant’s internal control over financial reporting.
- Management’s assessment of the effectiveness of the registrant’s internal control over financial reporting as of the end of the registrant’s most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. Any weaknesses in the internal control over financial activities that is identified by management must be disclosed.
- A statement that the registered public accounting firm that audited the financial statements included in the annual report containing the disclosure had issued an attestation report on management’s assessment. Also disclose any change to the internal control over financial reporting identified in connection with the evaluation that is likely to materially affect the registrants’ internal controls.

In some respects, the new requirements overlap existing FDIC guidelines for internal controls pertaining to insured institutions of \$500 million or more in total assets. However, the new mandate for disclosing material weaknesses and changes in control effectiveness represents a significant enhancement. The impact of this act on IT departments is that they must provide deep visibility into the companies’ finances, controls, operations and processes. To achieve this, some companies may have to implement entirely new systems. At the very least, IT must work with other departments to examine and update systems already in place.

USA Patriot Act

Approximately six weeks after the tragic set of events on September 11, 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). It contains strong measures to prevent, detect and prosecute terrorism and international money laundering. The Act is far-reaching in scope, covering a broad range of financial activities and institutions. The Act provides the groundwork for new filing and reporting obligations for financial institutions. It also requires certain additional due diligence and recordkeeping practices, especially in the area of private banking and foreign accounts. All financial services companies are covered under this regulation, and those supervised by the federal financial institution regulators or SEC will receive onsite inspections.

More specifically, Title III of the Act, captioned “International Money Laundering Abatement and Anti-terrorist Financing Act of 2001,” adds several new provisions to the Bank Secrecy Act (BSA). These provisions are intended to facilitate the prevention, detection and prosecution of international money laundering and the financing of terrorism. As required by the Act, the Federal financial institution regulators, in cooperation with the U.S. Treasury Department, established rules that require institutions to establish and document a customer-identification program (CIP). The CIP must meet the objectives outlined in the rules and represent a part of the institution’s anti-money laundering compliance program. The regulations specifically state the following:

A bank must implement a written Customer Identification Program (CIP) appropriate for its size and type of business that, at a minimum, includes each of the requirements of paragraphs (b) (1) through (5) of this section. If a bank is required to have an anti-money laundering compliance program under the regulations implementing 31 U.S.C. 5318(h), 12 U.S.C. 1818(s) or 12 U.S.C. 1786(q)(1), then the CIP must be a part of the anti-money laundering compliance program.

The USA PATRIOT Act further specifies that the CIP must provide for the following elements:

- Establish and document a CIP
- Obtain certain identifying information from customers
- Verify identifying information of customers
- Check customers against lists provided by federal agencies
- Provide notice to customers that information may be requested in the process of verifying their identities
- Produce and maintain records related to the CIP

The lack of an appropriate CIP and supporting records can be cited as a violation of federal law. The failure to ensure the integrity, availability and security of customer-verification data can result in the inability to demonstrate compliance. Immediate corrective action often results in higher costs and inefficient deployment of internal resources.

Other Laws and Standards Affecting Financial Services

In addition to the audit examinations and regulatory requirements previously described, there are a number of additional legal and compliance concerns affecting financial services companies. For example, there are mandates required by the governing bodies where the institutions conduct business. These may be at the state level, if within the United States, or placed into effect by other countries' governments.

A number of individual U.S. states have taken the initiative to enact laws addressing high-profile issues such as privacy and security—particularly with respect to customer financial information. One example is found in the California law, Civil Code 1798.82, in force since July, 2003. This law states that any person or business that deals with personal consumer information must disclose any unauthorized data access to the individuals affected as quickly as possible, and must remedy the cause of the breach.

Responsibilities in this area are also affected by regulatory requirements in other countries. For example, the 1995 European Union (E.U.) Data Protection Directive 95/46/EC prohibits the export of any personal data from the E.U. to countries that do not meet its minimum standards for consumer privacy protection. In May 2000, the U.S. and the E.U. approved the Safe Harbor Agreement that enables companies in the U.S. to continue to do business with the EU by compliance through closely supervised self-regulation.

Financial 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.

Regardless of the source, many of these requirements contain a similar set of guidelines as GLBA, Sarbanes-Oxley and the USA PATRIOT Act. These guidelines recommend companies have:

- Comprehensive, documented policies and procedures
- Procedures to test, evaluate and maintain appropriate internal controls
- Monitoring and reporting capabilities
- Oversight responsibility at the Board of Directors or Executive Management level

Furthermore, several of the federal agencies with regulatory enforcement responsibilities have joined together in an interagency task force to produce guidelines that provide extra definition in the areas of security-risk assessment and risk management and control. The guidelines state that companies must assess the likelihood of potential loss or destruction, along with the sufficiency of existing policy to control threats. In addition, companies must adopt security measures including:

- Access controls on customer information systems
- Access restrictions at physical locations
- Encryption of electronic customer information
- Procedures designed to ensure that system modifications meet security requirements
- Segregation of duties and employee-background checks
- Monitoring systems and procedures to detect attacks or intrusions
- Response programs that specify actions to be taken against unauthorized access
- Measures to protect against environmental hazards (floods, fire, etc.)
- Training staff to implement security programs

- Regular testing of key controls, systems and procedures

A very important point to remember is that none of the regulations is, by itself, a technical security standard. Even the interagency guidelines are broad in the role of an implementation specification. In order to define a security program that aligns with the general regulatory requirements, it's a good idea to look at security standards to serve as a framework.

One such security standard is outlined in ISO 17799. This standard originated in Great Britain, first as a national practice for information security. In 1998, this became the basis for specification BS 7799, which has gained wide acceptance throughout Europe and other countries where the British Commonwealth has influence (Canada, Australia, New Zealand and Hong Kong). In October 2000, the International Standards Organization adopted the code of practice of BS 7799 as the international security standard ISO 17799.

Adoption as an international standard has fueled acceptance across industries in other parts of the world, including the financial services industry in Asia. ISO 17799 contains the following ten working sections:

- Security Policy
- Asset Classification and Control
- Physical and Environmental Security
- Access Control
- Business Continuity Management
- Security Organization
- Personnel Security
- Communications and Operations Management
- Systems Development and Maintenance
- Compliance

The practices contained in these sections can form the basis for a security program to comply with industry regulations, along with setting the stage for a comprehensive corporate information security plan.

NetIQ Security Solutions

Even for security professionals, the array of security tools can seem dizzying. An organization might have one tool to perform technical compliance assessments and another for security monitoring. A third tool may provide log analysis, while another performs basic systems management functions. Perhaps another set of tools rolls out security patches and other updates to systems, while a whole other set of tools makes user management more effective.

NetIQ is uniquely positioned to provide highly effective security management solutions that work well together, but can also be implemented separately to address specific needs. These solutions fall into the following categories:

- Security policy management
- Vulnerability management
- Incident management
- Operational change control

- ☑ Compliance Reporting

Each of these categories and their respective solutions are described below.

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.

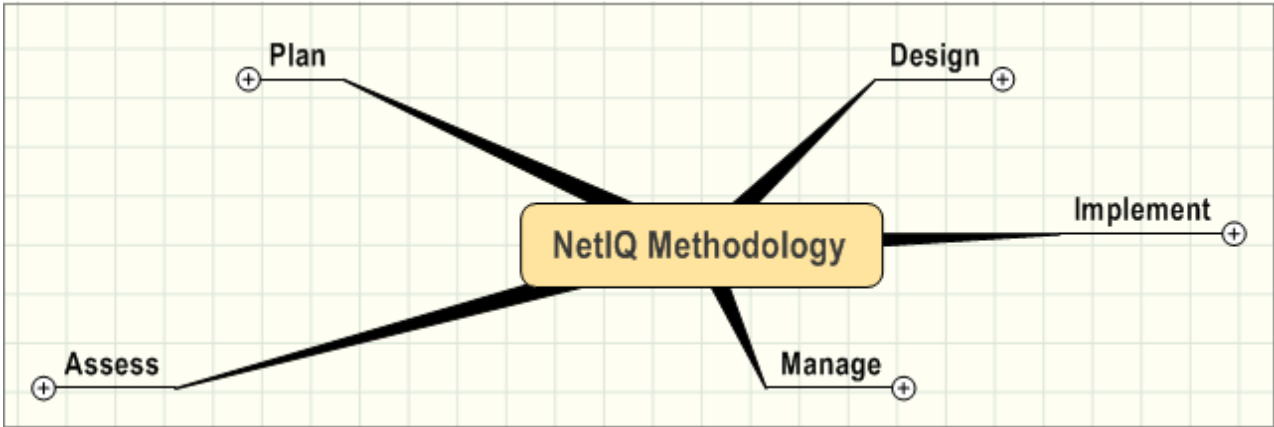
NetIQ Risk & Compliance Center

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

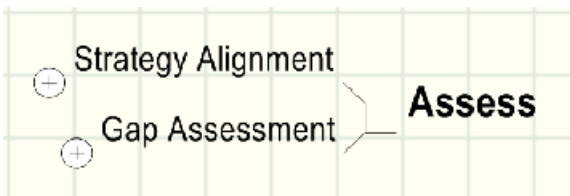
The NetIQ Risk and Compliance Center solution aligns security metrics gathered from your IT systems to demonstrate compliance with IT related policies and regulations and displays them in a customizable dashboard. This automated solution analyzes security assessment data and maps the results with government 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.

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. In each phase, NetIQ has the knowledge and resources available to assist customers in maximizing the effectiveness of their NetIQ products.



Assess

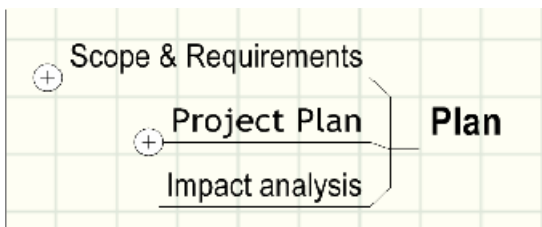


The initial step of the NetIQ methodology is to **assess** the current situation and parameters of the organization. This will create a baseline from which a plan can be put together and a design created, implemented, then operationalized for effective ongoing management by the organization. Assessment starts with identifying the strategy of the organization

and determining 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 government 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 aligned with 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 automated system.

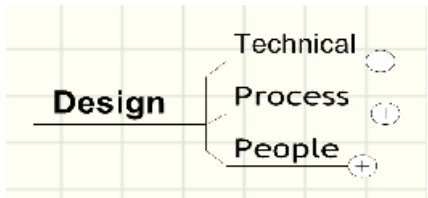
Plan



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.

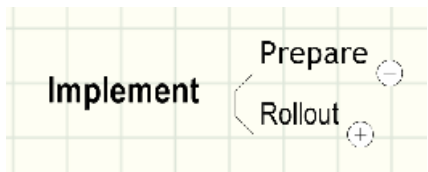
Design



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 are 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 secure assets.

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, 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 is available.

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 auditors 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 understanding how to interpret data and feed knowledge back into the automated functions of the products, or how to create enhanced reporting, NetIQ offers additional training or on-site consulting to ensure that the organization realizes the maximum possible benefit.

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 or call (888) 323-6768.

