NetIQ FISMA Compliance & Risk Management Solutions

The Federal Information Security Management Act (FISMA) requires federal agencies to create and implement a comprehensive information security program and report compliance to Congress' Office of Management & Budget (OMB) on an annual basis. Non-compliance could result in IT funding cuts for the agency.

Such regulatory requirements call for agencies to implement Managerial, Operational and Technical IT controls. It isn't enough to simply have mechanisms and personnel in place to deal with security problems, FISMA also requires that you must prove compliance with the required controls. Unfortunately, most agencies are experiencing difficulty translating the regulation in to specific tasks, much less demonstrating compliance.

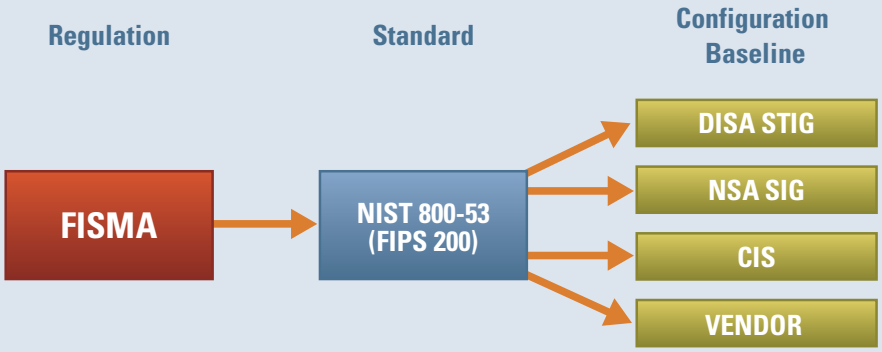
With NetIQ's new Knowledge-Based Service Assurance, agencies are offered a multi-pronged approach that enables them to measure and manage risk, remain compliant with corporate policies and new legislation, manage operational configuration and change and provide increased network security, availability and performance.

netiq

ACHIEVING FISMA COMPLIANCE

Information Security and Privacy regulations are purposely vague to ensure they cover a wide range of organizations over a long period of time without having to be amended by Congress. While this is necessary, it leaves organizations in the dark about how to ensure they are compliant with the regulation, so it is then up to the organization's management and security practitioners to determine how to comply. Compliance is aided by guidance from the enforcement agency or use of a generally accepted information security standard such as ISO 17799 or CobiT.

In the case of FISMA, it will eventually be the final publication of the National Institute of Standards & Technology's (NIST) Federal Information Protection Standard (FIPS) 200 that provides the necessary detailed guidance to federal agencies. Guidance is currently provided in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems." However, even these documents do not help an organization know exactly how to configure a particular system to ensure it is adequately secure. NIST thus recommends the use of platform-specific technical checklists from sources such as the Defense Information Systems Agency's Security Technical Implementation Guides (DISA STIGs), the National Security Agency's Security Information Guides (NSA SIGs), and the Center for Internet Security's Benchmarks (CIS). Many security software vendors and consultants also provide additional guidance.



UNDERSTANDING YOUR FISMA CHALLENGES

While agencies want to do the right thing, there are many challenges in complying with FISMA—from interpreting the regulation to providing the annual report to the OMB. Complying with FISMA can be both cost- and resource-prohibitive. In addition, auditing in the federal sector means overcoming a number of hurdles throughout the entire compliance process, including:

- >> Correctly balancing limited resources between FISMA compliance and other agency goals and mandates
- >> Objectively measuring compliance at the detailed control level consistently across systems
- >> Easily producing management and compliance-level reports on a regular basis
- >> Effectively creating a sustainable compliance process that operates efficiently year after year

To help you overcome these challenges, NetIQ offers a wide range of solutions designed around a comprehensive Policy Compliance and Risk Management methodology.

THE NETIQ SOLUTION

With NetIQ, you can assess your technical security posture, continuously ensure you operate within policy and implement cost-effective controls in your security environment to reduce risk and prove compliance.

To enhance security and meet your regulatory compliance needs, it is essential to address both the people and technology aspects of your environment. Every component of NetIQ's methodology contains elements of both, but at its simplest, Compliance and Risk Management can be thought of as a three-phase lifecycle centered around a Policy Framework, producing Metrics & Reporting for every aspect.

From developing your policy framework to automatically producing many of the metrics and reports you need to demonstrate compliance and reduce risk, NetIQ can help.

Assess - Before you can implement additional security controls, you must first understand what IT assets you have and which assets are FISMA-compliant. NetIQ Vulnerability Manager™ can help you with all aspects of the assessment phase and even includes DISA STIG, CIS and NetIQ FISMA Essentials templates to measure system compliance. VigilEnt™ Policy Center provides everything you need for your Policy Framework and to assess your people compliance.

Operate - While assessments are a beginning, in today's IT threat environment it is important to operationalize security processes so that you are continuously monitoring and addressing security issues. NetIQ Security Manager™ offers a complete solution in this area—from log management to security event monitoring to intrusion detection and management.

Control - Once you understand your organization's deficiencies, you can begin remediating issues or implementing compensating controls. For issues that are minor or where the cost of remediation is greater than the risk, you can either accept the risk or transfer it to a third party through insurance or outsourcing. NetIQ Vulnerability Manager and NetIQ Security Manager are embedded with remediation instructions and features to automate remediation and both can be used as compensating controls.

NETIQ'S CUSTOMIZED SOLUTIONS

While our general methodology provides you with a starting point for efficiently developing a Compliance and Risk Management solution, NetIQ understands that every agency and department has unique needs. NetIQ Professional Services has a staff of experienced consultants with MCSE, CISSP, ITIL and CCSA certifications and security clearances. In addition, we work closely with several partners whose primary focus is delivering services and systems integration to federal agencies. This expertise enables us to work closely with your organization to create a customized FISMA solution that addresses your agency's requirements and fits in with its IT systems and processes. The Services we offer include:

- >> Policy development and updates
- >> Technical design workshops
- >> Installation, configuration and roll-out of NetIQ products
- >> Customization of NetIQ products and integration with third-party products

NETIQ'S FISMA PRODUCTS

NetIQ's FISMA solution includes these best-of-breed products:

VigilEnt Policy Center is a web-based product for developing, approving and distributing any type of document in your policy and planning framework. A FISMA library is available, along with thousands of pre-developed policies written by renowned policy author Charles Cresson Wood. It enables you to meet numerous requirements, including the first control requirement under all 17 NIST 800-53 control families as well as all of your Awareness and Training requirements.

NetIQ© Security Compliance Suite - NetIQ Vulnerability Manager is a host-based configuration policy and vulnerability assessment tool. Use it to regularly run DISA STIG, CIS, or NetIQ FISMA Essentials templates to ensure that your systems are configured correctly and up-to-date on their security patches. You can also leverage NetIQ's real-time vulnerability feed from TruSecure can automatically test your systems for exposure or compromise by the latest exploits.

NetIQ Security Compliance Suite - NetIQ Security Manager provides continuous monitoring of all your security events. Consolidate and correlate security events from multiple IDS, network devices and software platforms in a single console. You can also collect security, event and audit logs for easy viewing, retention and analysis.

NetIQ Security Administration Suite™ enables you to easily manage your Active Directory and Group Policy environments. You can ensure that administrators have only the privileges they need, changes are properly authorized and tested before implementation and unauthorized changes are quickly detected.

MAPPING NETIQ'S PRODUCTS TO FISMA

This table provides you a quick view of how NetIQ products address each FISMA control family.

NIST 800-53		NetIQ Solutions		
Class	Control Family	Policy Center	Compliance Suite	Administration Suite
Managerial	Risk Assessment	X	X	
	Planning	X		
	System & Services Acquisition	X	X	
	Certification, Accredidation & Security Assessments	X	X	
Operational	Personnel Security	X		X
	Physical & Environmental Protection	X		
	Contingency Planning	X		
	Configuration Management	X	X	
	Maintenance	X		
	System & Information Integrity	X	X	
	Media Protection	X		
	Incident Response	X	X	
	Awareness & Training	X		
Technical	Identification & Authentication	X	X	X
	Access Control	X	X	X
	Audit & Accountability	X	X	X
	System & Communications Protection	X	X	

Contacts

Worldwide Headquarters

NetIQ Corporation
3553 North First Street
San Jose, CA 95134
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

NetIQ EMEA
+44 (0) 1784 454500
info-emea@netiq.com

NetIQ Japan
+81 3 5909 5400
info-japan@netiq.com
www.netiq.co.jp

NetIQ Australia & New Zealand
+61 2 9925 2100
www.netiq.com.au

For our offices in Latin America & Asia Pacific, please visit our web site at www.netiq.com/contacts

DS50172FMVM MB 0905