



eEye Digital Security®

Implementing a Successful Risk Assessment Strategy for Regulatory Compliance



Implementing a Successful Risk Assessment Strategy for Regulatory Compliance

The idea of security as a standard business process within an organization cannot be overstated.

Overview

Tighter controls and increasing accountability for corporate integrity have driven legislation that imposes significant new regulations on publicly traded corporations. A common component in these regulations is the oversight of technology and the role it plays in the organization. The result: supporting IT infrastructures must prove to be secure and resilient to variable circumstances. Specifically, two pieces of legislation can be addressed in part by implementing a comprehensive risk assessment strategy – the Sarbanes-Oxley Act of 2002 (Section 404) and the Gramm Leach Bliley Act of 1999 (The Safeguards Rule).

Sarbanes-Oxley Act of 2002

The Sarbanes Oxley-Act (SOX) is a set of complex regulations. Congress enacted this bill to restore confidence in public companies, where a plunging stock market, increased corporate fraud and numerous accounting scandals have had a negative impact on the economy. The Act has granted the SEC increased regulatory control, lengthened the statute of limitations and imposed greater criminal and compensatory punishment on executives and companies that do not comply.

SOX imposes significant new regulations on publicly held corporations. At least three sections in the law have serious implications for IT, effectively making IT management and clearly defined, measurable IT processes mandatory. SOX will affect how public organizations and accounting firms deal with corporate governance, financial disclosure and the practice of public accounting. Driven by the realities of today's global, inter-connected business environment, the impact of SOX is far reaching, affecting organizations and individuals across internal and external boundaries. Those affected include auditors, executive management, audit committees, attorneys, and even securities analysts, providing legislated guidelines for compliance that are applicable across disciplines related to financial reporting.

SOX Section 404

Section 404 of SOX delivers a mandate that all public organizations demonstrate due diligence in the disclosure of financial information and implement a series of internal controls and procedures to communicate, store and protect that data. Section 404 also requires organizations to protect these financial controls from internal and external threats and unauthorized access. This level of security is necessary to ensure companies maintain the highest data integrity for employees, customers and shareholders. Section 404 now means that each public company will need to develop an individualized approach to reporting and compliance. It will begin with a self-assessment of the internal controls the organization has around its financial reporting process. This self-assessment will typically involve internal stakeholders as well as an external audit firms who will work through a standardized framework to identify the gaps in compliance, as well as any associated security risks. This framework allows audit firms to map internal control objectives back to SOX requirements, allowing organizations to then apply process frameworks.

Gramm Leach Bliley Act of 1999

The Gramm Leach Bliley (GLB) Act of 1999 requires all financial institutions to ensure the security and confidentiality of customer's personal information. Within GLB, Section 501 of the Act specifically necessitates federal banking regulators to establish administrative, technical, and physical safeguards to protect customer information (e.g. names, addresses, phone numbers, Social Security numbers, bank and credit card numbers, income and credit histories, etc.) There are three principal parts to the privacy requirements of GLB, including: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.



Implementing a Successful Risk Assessment Strategy for Regulatory Compliance

The idea of security as a standard business process within an organization cannot be overstated.

The GLB Act gives authority to eight federal agencies and states to administer and enforce elements of GLB – most importantly, the Safeguards Rule. To consolidate guidance on this topic, the banking regulators jointly developed the “Interagency Guidelines” which require financial institutions to develop and implement information security programs. From the Interagency Guidelines, each agency has introduced and published further controls pertaining to the Safeguards Rule for businesses subject to their charter. The eight agencies include:

- Board of Governors of the Federal Reserve System
- Federal Deposit Insurance Corporation
- National Credit Union Association
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- Secretary of the Treasury
- Securities and Exchange Commission
- Federal Trade Commission

Each of the eight agencies have very similar guidelines pertaining to the safeguarding of customer information; therefore, the recommendations contained in this document are applicable to all organizations subject to GLB compliance. This document examines the Safeguards Rule in specific relation to the final document published by the Federal Trade Commission (16 CFR Part 314) and is intended to translate the safeguarding requirements into a simplified process that can be implemented using Retina®, eEye’s vulnerability assessment and remediation management technology as a baseline to simplify the process.

The Safeguards Rule

The GLB Safeguards Rule applies to companies of all sizes that are engaged in providing financial products or services to consumers. Under the Safeguards Rule, financial institutions must develop a formal written security plan that describes their program to protect customer information. As part of the plan, there are 5 elements that companies must comply with:

1. Designate one or more employees to coordinate the safeguards;
2. Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling risks.
3. Design and implement a safeguards program, and regularly monitor , test and manage that program.
4. Select appropriate service providers and contract with them to implement safeguards.
5. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business arrangements, operations, or the results of testing and monitoring the safeguards.

From the above list, a bulk of the effort required to attain GLB compliance rests with steps two and three: Identifying and assessing risks as well as designing and implementing a comprehensive safeguards program. While there are a variety of methodologies that can be utilized for risk assessment, the process of risk identification and remediation go hand-in-hand. eEye’s Enterprise Vulnerability Assessment solution incorporates all of these process-driven elements into a simplified program of identification and risk reduction which meets GLB requirements.

Implementing a Successful Risk Assessment Strategy for Regulatory Compliance

The idea of security as a standard business process within an organization cannot be overstated.

Attaining Regulatory Compliance via eEye's Enterprise Vulnerability Assessment and Remediation Management Solution

Utilizing a proven enterprise vulnerability assessment and remediation management solution, organizations subject to regulatory requirements can automate a majority of these requirements associated with the risk analysis process - from the asset identification and auditing phase, through the review and remediation stage, to final verification of fixes. Eye's complete Enterprise Vulnerability Assessment and Remediation Management solution incorporates eEye's Retina Network Security Scanner and REM Security Management Console to manage the process and minimize the resources needed to attain proper compliance.



Vulnerability Assessment & Remediation Management Workflow

The idea of security as a standard business process within an organization cannot be overstated. A computer security audit is a systematic, measurable technical assessment of how the entity's security policy is employed. Security audits do not take place in a vacuum. They are part of the ongoing methodology of defining, maintaining and improving effective security throughout an organization. Following an established vulnerability assessment and remediation management process is a proven approach to attaining network security for regulatory compliance. Network security best practices can be illustrated by an integrated, continuous vulnerability management workflow comprised of six distinct steps: Discover; Audit; Delegate; Remediate; Report; and Adapt.

Step 1: Discovery

In order for organizations to properly assess network security, it is important to understand the digital assets that make up the network. Discovery is an important first step in identifying, checking and tracking all of the servers, workstations, and devices that are attached to the network.

With the ability for data to go mobile or wireless, the importance of Discovery is greatly enhanced. It is vital to identify any rogue systems and devices that can find their way into the network. Laptop computers, PDAs, MP3 players, thumb drives, no matter how well intentioned they are, can put your network at risk and must be identified and audited. A quality security scanner can identify and map all of these known and rogue assets in a centralized database, giving you a comprehensive map of your network.

Step 2: Audit

The vulnerability audit is the linchpin of the entire vulnerability management process. It entails checking all operating systems hardware configurations, and application configurations as well as checking for any policy infractions. The vulnerability scanner used to audit must be able to check all direct attached systems and devices, as well as any wireless and mobile devices within the network. It needs to feature an up-to-date, comprehensive database of known vulnerabilities that will help to ensure all vulnerabilities are properly identified.

Vital to the scanning process is the backing and support of a dedicated research team that actively works to keep the scanner on pace with the growing number of vulnerabilities being identified daily. The eEye Research Team, for example, is unrivaled in its track record for identifying high-risk vulnerabilities, alerting customers, and working with vendors for effective patches.

Implementing a Successful Risk Assessment Strategy for Regulatory Compliance

The idea of security as a standard business process within an organization cannot be overstated.

Step 3: Delegate

Upon completion of a given vulnerability assessment, remediation activities can be prioritized and assigned to team members. Rules can be created to automatically delegate security events as tasks according to severity level, origin or vulnerability type. It is important to prioritize based on the nature of the vulnerability itself: how likely is it to be attacked; what are the methods that might be used; and so on. A second aspect of prioritization is the business use and criticality of the asset. If the asset is vulnerable, what are the implications of it being compromised? What data is stored there? What applications are running it?

Step 4: Remediate

For smaller organizations, the stand-alone capabilities within some of the network security scanners may be sufficient to meet the delegation needs of IT and network security personnel. More detailed requirements, though, will need to be addressed by remediation-specific products. These solutions can automate and simplify the process of assigning, tracking and reporting on remediation progress. Purchased either as part of a vulnerability management suite or standalone, the best solutions can be integrated easily into an IT environment. For large, distributed environments with expansive networks, enterprise-level solutions can provide vulnerability remediation as part of an integrated end-to-end vulnerability management solution.

The top remediation solutions provide hands-on fixes that resolve issues correctly – the first time. Remediation management products should also provide detailed remediation instructions to guide administrators through the process of correcting network vulnerabilities before an attacker can compromise them. After a patch or fix has been applied, a follow-up scan can serve as verification that the issue has been addressed and corrected.

Step 5: Report

Reporting, trend analysis, policy settings, resource management, and customization are all part of the Report step of the integrated vulnerability management process. Reporting is a very important aspect that IT organizations have come to rely on. The ability to dissect the data in ways most relevant to a specific organization is critical to educating and communicating to constituents. Whether monitoring specific machine information, providing executive level views or communicating other important data, reporting is an important element that must be evaluated along with everything else.

Step 6: Adapt

Likewise, the ability to modify scans, insert custom checks into the database, address specific machines and groups, or to customize in some other fashion is critical to assuring the most secure network environment. The more you go through the process, the more you will understand the specific nuances of managing vulnerabilities within your specific environment. Once you analyze the data, you must be able to apply the knowledge you gain back into your vulnerability management process. The Report and Adapt stages provide the necessary documentation to prove that the proper security measures for HIPAA are being completed and maintained on a regular, ongoing basis.

Implementing a Successful Risk Assessment Strategy for Regulatory Compliance

The idea of security as a standard business process within an organization cannot be overstated.

About Retina Network Security Scanner

Retina Network Security Scanner is recognized as the #1 rated network vulnerability assessment scanner. Retina sets the standard in terms of non-intrusiveness, speed, ease of use, reporting, and advanced vulnerability detection capabilities. For small organizations seeking to attain GLB compliance, Retina is the perfect stand-alone software to perform risk assessments to identify and correct network vulnerabilities.

About eEye's Retina Enterprise Suite

In a larger organization, attaining compliance is much more difficult without an enterprise-wide solution to facilitate the entire risk assessment process. eEye's Retina Enterprise Suite incorporates Retina Network Security Scanner, Retina Remediation Manager and the REM Security Management Console to thoroughly address vulnerability management and regulatory compliance in large scale, complex and/or distributed environments.

Retina Enterprise Suite uniquely combines advanced security technology with best practices vulnerability management workflow process to provide the most effective compliance remedy. An enterprise-class solution, Retina Enterprise Suite enables security and IT professionals to create and enforce security policies, establish roles and responsibilities, perform regular audits, remediate issues, verify corrective actions, and report on the entire network threat reduction process. Retina Enterprise Suite centralizes the security events management process into one complete solution and streamlines the regulatory compliance process.



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276

