

Safeguarding Financial Information and Ensuring Compliance

SECNAP® Network Security has been a trusted partner to financial institutions since 2001 for our ability to address and remediate the distinctive needs of this highly regulated community. Leveraging our comprehensive portfolio of services, CIOs, CISOs, network and IT managers have been able to dramatically reduce vulnerabilities and enhance protection for their sensitive data—and institutions governed by the **Gramm-Leach-Bliley Act** and other financial legislation have substantially improved their compliance positions.

Failure to comply with regulatory standards can result in the exploitation of vulnerabilities by hackers and other cybercriminals. Identities may be stolen and sensitive or private information abused for malicious profit. Data breaches have far-reaching impacts, and in 2010 cost the average U.S. organization \$7.2 million per breach in terms of remediation, notification and customer churn, according to the Ponemon Institute. In the financial industry, 95 data breaches were reported to the Privacy Rights Clearinghouse in 2010, exposing 6.3 million records of depositors, clients, employees and other stakeholders.

Periodic security assessments are a requirement, not just for compliance but for sound business practice as well. SECNAP offers a full complement of network security solutions designed to meet your needs today and tomorrow.

Tools & Expertise

In addition to their extensive hands-on experience, our professionally certified network security auditors leverage a complete tool kit in order to evaluate risk in your organization and make practical recommendations for remediation. Tools may include automated testing, personnel interviews, policy reviews, procedural and process evaluations, in-depth analyses and more.

Our auditors review security practices in the context of your current business requirements and future objectives—a strategic approach that enables you to address vulnerabilities cost-effectively.

Our final audit report provides a thorough assessment of vulnerabilities, which are described in detail, ranked in terms of risk, and accompanied by expert recommendations to help you address them. Remediation assistance is available on request.

Features & Benefits

The most significant benefit of a GLBA Assessment is the peace of mind you'll gain knowing that Gramm-Leach-Bliley Act requirements have been met, as well as those suggested by the Offices of Thrift Supervision and Controller of the Currency. The SECNAP GLBA audit will also:

- ***Create a GLBA compliance benchmark for your organization, or provide a fresh third-party assessment.***
- ***Identify strengths and weaknesses of current security practices, especially those protecting Non-Public Personal Information.***
- ***Prioritize exposures according to level of risk for IT convenience in addressing them.***
- ***Deliver remediation recommendations consistent with compliance regulations, corporate policy, and best practices in the financial industry.***
- ***Provide a repeatable methodology to facilitate periodic GLBA audits.***
- ***Prevent your organization from becoming a Privacy Rights Clearinghouse statistic.***

GLBA Assessment

The SECNAP GLBA Assessment consists of the following reviews and testing.

Interviews and Reviews

- Conduct interviews and review audit questionnaire with senior IT management
- Review Internet use policies
- Review current security exception handling procedures
- Review current Firewall rules
- Review laptop and remote access security methods

Preparation of Full Network Map

(IP address and services assessment)

- Install SECNAP Internal Vulnerability Assessment Scanning (IVAS) appliance to monitor network
- Develop list of all servers, hosts and services resident on network
- Perform external penetration and vulnerability tests on all external IP addresses
- Perform internal vulnerability tests on all IP devices on network
- Complete full port scan for every external IP address on network
- Select and execute from suite of nearly 40,000 specific tests available
- Test user password policy

Procedural Review

- Review written IT security policies in detail and compare to actual implementation
- Review physical security procedures and compare with written policies
- Interview senior members of corporate staff relative to security awareness and policy implementation
- Check authorization controls to ensure they are being followed and are effective in preventing unauthorized information access
- Review incident response process to ensure necessary controls are in place to contain incidents and minimize damage once an incident is recorded

Compliance Requirements Review

- Review results of IT and procedural audits in relation to applicable GLBA regulations
- Review security management processes to ensure policies are being followed
- Review administrative procedures, physical safeguards and technical security mechanisms to confirm they are adequate to ensure compliance

Upon completion of the GLBA Assessment, these information and remediation tools will be delivered:

Executive Summary

At the executive level, we report on where you stand objectively as well as relative to other companies in your industry, and outline steps that can be taken to improve your security profile and reduce your risk.

Results of penetration and vulnerability testing are highlighted. An outline of possible employee abuses or violations of your use and security policies is provided.

Detailed Findings Report

This detailed report is targeted to staff who are responsible for GLBA compliance as well as the IT team, and is accompanied by detailed backup including scan results. The report assists stakeholders in understanding the identified vulnerabilities and risks, as well as the suggested remediation steps. If severe or critical issues are found, our audit team can recommend solid strategies to help you reduce risk to a level that is acceptable for your organization.

The report outlines recommendations for changes to written security and Internet use policies, security handling procedures, employee training, and any additional measures to bring your company up to the best security practices for your industry and security profile.

At the close of our work, you will have a complete picture of current vulnerabilities with respect to requirements of the Gramm-Leach-Bliley Act as well as the steps you can take to address them. You'll possess the information necessary to ensure that your security program is GLBA-compliant, and earn some well-deserved peace of mind in the process.



866-732-6276
www.secnap.com