



## VULNERABILITY MANAGEMENT FOR GLBA COMPLIANCE

### GLBA Defined

Gramm-Leach-Bliley is U.S. Public Law 106-102 – the Financial Services Modernization Act of 1999 (GLBA, or “the Act”). Congress created the Act to improve consumer financial services by opening up competition between banks, securities and insurance companies. The complex, seven-Title law applies to about 9,500 financial institutions. Compliance is mandatory; non-compliance can trigger civil liability and penalties to institutions, and personal liability and penalties to officers and directors.

### Digital Security Is Part of the GLBA Process

Security is a crucial part of protecting consumers’ personal nonpublic information processed electronically by financial institutions under GLBA. According to the Act’s Safeguards Rule, they must:

- Ensure security and confidentiality of customer information.
- Protect against anticipated threats or hazards to security or integrity of information.
- Protect against unauthorized access to or use of the customer information.

The Act requires financial organizations to create a comprehensive, written Information Security Program. Guidelines specify seven steps for development and implementation, and nearly all require ongoing risk assessment.

### QualysGuard Meets Key GLBA Compliance Rules

The QualysGuard vulnerability management and policy compliance solution helps financial institutions to meet many key security guidelines detailed in the GLBA Safeguards Rule at 12 CFR Part 30, Appendix B, Sec. III.; see back page for details.

### Automation Makes Compliance Easier and Cost Effective

As an on demand web service, QualysGuard enables immediate compliance with key GLBA security guidelines by allowing subscribers to automatically discover and manage all devices and applications on the network, identify and remediate network security vulnerabilities, measure and manage overall security exposure and risk, and ensure compliance with internal and external policies for GLBA. The combination of internal and external audits provides the most comprehensive, GLBA-compliant assessment of risks to unauthorized access of nonpublic financial data. QualysGuard can also monitor GLBA compliance by associated service providers, subsidiaries and other affiliates.

*“By showing the FDIC our QualysGuard reports, we prove that we regularly identify risks, rank them by priority, adjust our actions to eliminate those risks, and then verify that we’re no longer vulnerable.”*

Lenard East,  
VP Network Engineering & Operations  
**Bank of the West**

*“Not only do we use QualysGuard to perform all of our vulnerability assessments, it also helps us demonstrate compliance with financial regulations and manage overall business risk.”*

Daniel Hereford,  
Data Security Officer  
**First Bank & Trust**



## Vulnerability Management for GLBA Compliance

QualysGuard capabilities directly address many key safeguards required by GLBA. These safeguards are based on Interagency Security Guidelines developed by the banking industry. The matrix quotes excerpts from GLBA security guidelines at 12 CFR Part 30, Appendix B, Sec. III, and associates each with QualysGuard capabilities.

GLBA REQUIREMENTS	QUALYSGUARD CAPABILITIES
<b>Assess Risk</b> – Each bank shall: “ <u>Identify reasonably foreseeable internal and external threats</u> that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.” (B)(1)	QualysGuard tests your network with the industry’s largest, most up-to-date database of security vulnerability audits
<b>Assess Risk</b> – Each bank shall: “ <u>Assess the likelihood and potential damage of these threats...</u> ” (B)(2)	QualysGuard automatically prioritizes vulnerabilities to help you identify the biggest security risks
<b>Assess Risk</b> – Each bank shall: “ <u>Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.</u> ” (B)(3)	Using QualysGuard for regular network scans helps you instantly assess the repellant capability of security policy
<b>Manage and Control Risk</b> – Each bank shall: “ <u>Regularly test the key controls, systems and procedures of the information security program.... Tests should be conducted or reviewed by independent third parties</u> or staff independent of those that develop or maintain the security programs.” (C)(3)	The third-party QualysGuard web service provides you with unlimited scans 24x7 – a Guideline-compliant compliment to every security program
<b>Oversee Service Providers</b> – Each bank shall: “ <u>Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines;</u> ” (D)(2)	Financial institutions can direct service providers to use QualysGuard to satisfy this Gramm-Leach-Bliley Act Guideline
<b>Oversee Service Providers</b> – Each bank shall: “ <u>...monitor its service providers to confirm that they have satisfied their obligations as required by section D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.</u> ” (D)(3)	Financial institutions can use QualysGuard to monitor and test networks of service providers for compliance with security Guidelines
<b>Adjust the Program</b> – “Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any <u>relevant changes in technology</u> , the sensitivity of its customer information, internal or external threats to information, and the bank’s own <u>changing business arrangements</u> , such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.” (E)	QualysGuard helps financial institutions to instantly react to any change in security technology, new threats, and new business arrangements
<b>Report to the Board</b> – “Each bank shall report to its board or an appropriate committee of the board at least annually. <u>This report should describe the overall status of the information security program and the bank’s compliance with these Guidelines. The reports should discuss material matters</u> related to its program, <u>addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management’s responses; and recommendations for changes in the information security program.</u> ” (F)	Security data revealed by powerful QualysGuard reporting capabilities presents a comprehensive, organized snapshot of a network’s security risks, easily understood by executive level managers
<b>Implement the Standards</b> – “Each bank <u>must implement</u> an information security program pursuant to these Guidelines by July 1, 2001. (A grandfathering of agreements with service providers expire on July 1, 2003.) (G)(1 and 2)	As a web service, QualysGuard requires no special installation or provisioning; users get immediate compliance adhering to these Guidelines



**USA – Qualys, Inc.**  
1600 Bridge Parkway  
Redwood Shores  
CA 94065  
T: 1 (650) 801 6100  
sales@qualys.com

**UK – Qualys, Ltd.**  
224 Berwick Avenue  
Slough, Berkshire  
SL1 4QT  
T: +44 (0) 1753 872101

**Germany – Qualys GmbH**  
München Airport  
Terminalstrasse Mitte 18  
85356 München  
T: +49 (0) 89 97007 146

**France – Qualys Technologies**  
Maison de la Défense  
7 Place de la Défense  
92400 Courbevoie  
T: +33 (0) 1 41 97 35 70

