



Gramm-Leach-Bliley Act Protecting the Privacy of Customer Information

Table of Contents

Purpose
Overview
Gramm-Leach-Bliley Act (GLBA)
Supplemental GLBA Guidance
GLBA Security Objectives
Failure to Comply
Enhanced IAM Security Guidelines



www.centuric.com

Toll Free: 1.866.376.6767 ▪ Main: 954.691.1669 ▪ Fax: 954.691.1689
6682 NW 16th Terrace ~ Fort Lauderdale, FL 33309 USA

Centuric, the Centuric logo, and other trademarks, service marks, and logos are registered or unregistered trademarks of Centuric, LLC and its subsidiaries in the United States and other countries. All other trademarks belong to their respective owners. All rights reserved. 02/2008

Purpose

MSMR Business Solutions has prepared this white paper as ongoing training and to help your institution comply with the Gramm-Leach-Bliley Act by raising your awareness of:

1. Potential penalties for non-compliance
2. Key GLBA Data Protection rule mandates
3. Operational areas that require heightened risk focus under GLBA

Overview

Information is one of the most important assets of an institution. Protection of information assets is necessary to establish and maintain trust between an institution and its customers. Timely and reliable information is important to process transactions and support an institution and customer decisions.

Effective administrative, physical, and technical security measures must be in place to guarantee a consumer that his or her information and privacy are protected. On a broad scale, industries have a responsibility of protecting the nation's institutional services infrastructure. The security of systems and information is paramount to the safety and soundness of an organization and to the privacy of customer information.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), passed in 1999, has defined a framework of administrative, physical, and technical safeguards that must be implemented to:

1. Ensure the security and confidentiality of customer information
2. Protect against anticipated threats or hazards to such records
3. Protect against unauthorized access to or use of customer information which could result in harm or inconvenience to the customer

The GLBA spans a broad range of industries. Organization's affected by the GLBA include banks, mortgage brokers and lenders, financial planners, credit card companies, security firms, insurance agencies, tax preparers, real estate agencies, and others.

Effective July 2001, all federally insured financial institutions must be able to continuously demonstrate that they have a Board-approved compliant security program in place and it is being maintained regularly.

Supplemental GLBA Guidance

In early 2003, the federal regulatory banking agencies issued supplemental GLBA guidance to communicate additional detailed requirements of a heightened risk focus for information security.

The combined requirements of the GLBA Data Protection Rule and the supplemental Federal Financial Institutions Examination Council (FFIEC) guidance defines the framework for financial institutions to follow in establishing a safe, sound and secure information security infrastructure.

More often than not, organizations incorrectly perceive information security as the state or condition of controls at a point in time. Security is an ongoing process. An institution establishes and maintains highly effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk

tolerance levels. Institutions protect their information by establishing a security process that *identifies* risks, forms a strategy to *manage* the risks, *implements* the strategy, *tests* the implementation, and *monitors* the environment to control the risks.

A copy of the supplemental GLBA guidance can be obtained on our website at http://www.msmsolutions.com/guidelines/information_security.pdf

GLBA Security Objectives

1. Information security risks must be assessed utilizing a formal process to identify vulnerabilities, threats, and attacks, as well as the probability of their occurrence and outcomes.
2. A security strategy needs to be in place to mitigate risks. The plan must integrate technology, policies, procedures, and training.
3. The Board and Senior Management must be actively involved in overseeing the security program.
4. Regular Board reporting is required on an annual basis at a minimum.
5. The acquisition and operation of technology to control security must be implemented.
6. In order to maintain security control at the appropriate risk level, duties and responsibilities must be assigned to managers and staff members. The individual must understand their roles and responsibilities and have the knowledge to fulfill them.
7. Institutions must provide Board Members, Management, and Staff Members an avenue for continual training and education.
8. Organizations must use various security testing methodologies to gain the assurance that risks are properly assessed and mitigated.
9. Vendors must be overseen to ensure that they are meeting their obligations.
10. The security program needs to be continuously monitored. Information regarding new threats and vulnerabilities needs to be analyzed. This information should be used to update the risk assessment and the security strategy and controls.

Failure to Comply

Compliance with the GLBA is mandatory. An institution that does not meet the security requirements is subject to enforcement and liability exposure. Failing to comply includes up to \$1,000,000.00 in fines, enforcement actions, and other penalties.

A financial institution that is deemed deficient or non-compliant in its administrative, physical, and/or technical safeguard is subject to enforcement measures by the regulatory agencies.

The potential liability for noncompliance is astounding.

Enforcement measure examples:

1. FDIC insurance can be terminated
2. Corporate officers can be removed from positions and permanently barred from working in the banking industry. They can also be fined up to \$1,000,000.00 and held liable for civil penalties of up to \$10,000.00

Please note, that on April 7, 2003 the Office of the Comptroller of the Currency (OCC) announced civil money penalty enforcement actions against two bank employees who violated the GLBA rules.

Enhanced IAM Security Guidelines

MSMR Business Solutions uses the following guidelines to perform the enhanced IAM security assessment:

1 - Baseline Activities

- 1) INFOEC Documentation
 - a) Policies
 - b) Guidelines/requirements
 - c) System Security Plans (SSP)
 - d) Standard Operating Procedures (SOP)
 - i) User system security manuals
- 2) INFOSEC Roles and Responsibilities
 - a) Upper Level Management
 - b) Systems Operation
 - c) User Community
- 3) Identification & Authentication
 - a) Password characteristics
 - i) Minimum length
 - ii) No dictionary words
 - iii) No common association
 - iv) Alpha/numeric/special character combination
 - v) Upper/lower case sensitive
 - vi) Numeric not first or last
 - vii) User chosen / machine generated
 - viii) Password expiration
 - ix) User change capability
 - x) History file
 - xi) Classification
 - xii) Group accounts (shared passwords)
 - b) Password management consistency
 - i) Protected password files
 - ii) No auto-logon script
 - iii) Training and awareness
- 4) Account Management
 - a) Documented account management policy and procedures
 - b) Written formal account request
 - i) General and privileged user agreements
 - ii) Supervisor and data owner approval for access
 - iii) Minimal privilege access
 - c) Account initialization
 - d) Account termination
 - e) Account maintenance
 - f) Special accounts
- 5) Session Controls
 - a) Protected, logged on workstation
 - b) Time-outs
 - c) Lock-screen capability with password
 - d) Warning banner
 - e) Lock-out after Unsuccessful logon attempts
 - f) Account history banner

- g) Forgotten password/lock-out re-initialization
- h) Limited use of privileged accounts

2 - External Connectivity

- 1) Internet policy
 - a) Firewall control
 - b) Limit applications/ports
 - c) Individual authentication to firewall
 - d) Audit Firewall activity
- 2) Firewall boundaries
- 3) Hide internal architecture
- 4) Multiple firewalls for internal controls
- 5) Modems
 - a) Policy
 - i) Restricted modem use
 - b) Formal justification for modem access
 - c) Dial in/dial out capability
 - d) Security Features
 - e) Termination of remote access at departure
 - f) Modem disconnect after inactivity
 - g) Regularly monitor modem use
- 6) Dedicated Connectivity
 - a) Policy/Memorandum of agreement
 - b) Backdoor connectivity

3 - Telecommunications

- 1) Documented requirements and procedures for transmitting classified and sensitive information
- 2) Encryption issues – Purpose (confidentiality, integrity, non-repudiation)
 - a) Trust in communications medium
 - b) Strength of algorithm
 - c) Alternate routes for increased availability

4 - Auditing

- 1) Policy requiring mandatory auditing
- 2) SOP defining what to audit
- 3) Audit analysis and reporting on timely basis
- 4) SSA trained in audit analysis

5 - Vulnerability Assessment

- 1) Internal scans
- 2) External scans

6 - Virus Protection

- 1) Policy
- 2) Personal software loaded with SSA approval
- 3) Scan incoming software
- 4) System scans
- 5) Update tools
- 6) Employee education/training

7 - Contingency Planning

- 1) Documented
- 2) Identify mission or business critical functions
- 3) Uninterruptible Power Supply (UPS)
- 4) Identify responsibilities
- 5) Coordinated with the System Security Plan
- 6) Maintained onsite and off-site
- 7) Periodic scheduled testing

8 - Maintenance

- 1) Policy and procedures
- 2) Personnel clearance level
- 3) Control of diagnostic software
- 4) Remote maintenance access
- 5) Preventative maintenance
- 6) Maintenance records

9 - Configuration Management

- 1) Current system diagrams
- 2) List of all system resources
- 3) Control of relocation and reconfiguration of system resources

10 - Back-ups

- 1) Documented in SSP and SOP
- 2) Schedule
- 3) Proper storage
- 4) Periodic testing of back-ups

11 - Labeling

- 1) Policy/SOPs
- 2) Document what/why information is classified and/or sensitive
- 3) Employees trained on proper marking procedures
- 4) Removable media
- 5) System components

12 - Media Sanitization /Disposal

- 1) Documented policy and SOPs
- 2) Media sanitization methods
- 3) Establish responsibilities
- 4) User education / training
- 5) Contract concerns

13 - Physical Environment

- 1) Physical environment can be used to offset lack of system security capabilities
- 2) Ramifications to INFOSEC posture

14 - Personnel Security

- 1) Background checks
- 2) Security clearance

- 3) Signed user agreements
- 4) Employee awareness of social engineering techniques

15 - Training and Awareness

- 1) Users are usually the weakest link in security
- 2) Documented responsibilities

About Us

Centuric offers a comprehensive suite of products and services tailored to address the complex issues facing businesses today. Some of our main areas of expertise include Network Support Consulting Services, STORServer® Managed Data Services, Infrastructure Buildout and De Novo Services.

Centuric offers great value to its clients. In business since 2001, we employ a highly credentialed staff of professionals who deliver exceptional client service. Our company is nimble enough to react quickly to market changes, and we use the latest proven technologies. We have extensive regulatory compliance expertise. We also offer options for no capital expenditures through our managed services solutions. And our dedicated support and Help Desk personnel are always available to assist our clients.

For these reasons – and more – the 2008 South Florida Business Journal recently honored Centuric with a listing in four of its “Top 25” categories:

- Fastest Growing Private Companies
- Fastest-Growing Technology Companies
- Largest IT Consultant Firms
- Largest Computer Networking Companies

Centuric uses a federally recognized standard methodology to help our clients meet compliance and mitigate security risks. We have staff certified by the National Security Agency (<http://www.nsa.gov/>) utilizing INFOSEC Assessment Methodology (IAM). Our enhanced IAM methodology encompasses the GLBA requirements as well as the responsibility to protect institutional information and systems infrastructure.

Our Mission Statement

Centuric is focused on improving our clients’ business performance by providing technology solutions. Our core portfolio comprises on-site and remote support, managed services, systems integration and business applications. Our purpose and passion is to provide signature service that consistently exceeds client expectations.

Contact Information

Centuric, LLC
6682 NW 16th Terrace
Fort Lauderdale, FL 33309 USA
954.691.1650
411@centuric.com
Toll Free 1-866-376-6767
<http://www.centuric.com>

*White Paper / January, 2004
Revised February, 2008*



www.centuric.com

Toll Free: 1.866.376.6767 ▪ Main: 954.691.1669 ▪ Fax: 954.691.1689
6682 NW 16th Terrace ~ Fort Lauderdale, FL 33309 USA

Centuric, the Centuric logo, and other trademarks, service marks, and logos are registered or unregistered trademarks of Centuric, LLC and its subsidiaries in the United States and other countries. All other trademarks belong to their respective owners. All rights reserved. 02/2008



www.centuric.com

Toll Free: 1.866.376.6767 ▪ Main: 954.691.1669 ▪ Fax: 954.691.1689
6682 NW 16th Terrace ~ Fort Lauderdale, FL 33309 USA

Centuric, the Centuric logo, and other trademarks, service marks, and logos are registered or unregistered trademarks of Centuric, LLC and its subsidiaries in the United States and other countries. All other trademarks belong to their respective owners. All rights reserved. 02/2008