

GLBA Information

The Gramm-Leach-Bliley Financial Modernization Act

Overview information

In 1999, Congress eliminated barriers that had restricted the types of products and services that banking institutions could offer. GLBA enabled financial institutions and their affiliated companies to engage in a broad range of commercial activities including things like insurance, securities, real estate, property appraisals, tax preparation, and debt collections.

The same act of Congress imposed strong confidentiality constraints on institutions that offered products/services with a financial flavor/character. The intent was to insure the absolute security and confidentiality of customer data.

GLBA views “customers” as individuals/households, not as business entities. The security constraints pertain to this type of customer information: names, addresses, phone numbers, social security numbers, account numbers, credit histories, transaction content, and the like.

Implications specific to IT management

GLBA compliance clearly includes managing information within computer systems. The rules specifically mention the following computer system elements: network design, software design, data processing, data storage, data transmission, and data disposal.

Enterprises within the jurisdiction of GLBA must evaluate the effectiveness of safeguards intended to protect the confidentiality of customer data. This assessment must be conducted within enterprise operations that can gain access to customer records. From the viewpoint of IT management, the assessment action plan must incorporate these principal features:

- A. Identify potential internal/external risks to the security, confidentiality, and integrity of customer information so as to protect against unauthorized access/use/disclosure/ alteration/destruction of information which could harm or inconvenience a customer.
- B. Design, implement, and maintain comprehensive information safeguards to control vulnerabilities identified through a risk assessment.
 - ⊕ These security safeguards must include administrative, technical, and physical safeguards.
 - ⊕ The safeguards must be capable of detecting and responding to attacks, intrusions, or other systems failures.
- C. Assess the sufficiency of computer system safeguards by regularly testing/measuring the effectiveness of the key controls and procedures.

How Unbeaten Path can help

Two of our software products hit the bulls-eye on GLBA compliance for the iSeries platform.

- ☑ **Bill of Health**™ provides 50 robust assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability.
- ☑ **Stitch-in-Time**® **Data Integrity Software** observes and saves information about irregular data modification activities. It tells your security officer: 1) WHO did it, 2) exactly WHAT they did, 3) precisely WHEN they did it, and 4) HOW they did it. It even catches someone smart enough to think that they can defeat audit strategies.

Enterprises within the jurisdiction of GLBA

The following information provides more definition about the types of enterprises or institutions that must comply with the GLBA rules. The first definition appears to be the broadest; there is some overlap across the four definitions. Click on any of the “go-see-it” links to directly access information provided by the federal government:

- Enterprises engaging in activities that are financial in nature – [go-see-it](#)
- Financial holding companies – [go-see-it](#)
- Non-banking activities and acquisitions by bank holding companies – [go-see-it](#)
- Residential real estate settlement services – [go-see-it](#)

Here’s the full text of the final GLBA rules

Here is the Federal Register publication of the final rules pertaining to the “Privacy of Consumer Financial Information.” This is known as “Subtitle A” of the Act and is dated May 24, 2000. [go-see-it](#) Brace yourself for a 45 page .pdf download.

Here is the Federal Register publication of the final rules pertaining to “Standards for Safeguarding Customer Information.” This is known as “Subtitle B” of the Act and is dated May 23, 2002. This is the part of the act which describes the manner in which the Subtitle A objectives must be implemented. [go-see-it](#) This .pdf is only 12 pages.

Page 2 of 2

Return to the [IT Security Assurance](#) page