May 23, 2003 *-- The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act, becomes effective today. As of today, financial institutions subject to the Rule must have in place a comprehensive security program to ensure the security and confidentiality of customer information.*[1]

Do You Know if You are in Compliance?

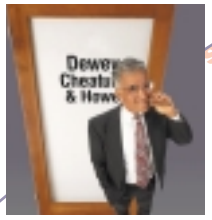
www.newera.com

What Your IT Audit Staff Should Know about GLBA

GLBA – Gramm Leach Bliley Act

The Financial Modernization Act, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.



The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, which receive such information. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions. [2]

To implement its information security program, each financial institution must:

- Designate an employee or employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and assess the sufficiency of any safeguards in place to control the risks;
- Design and implement safeguards to address the risks and monitor the effectiveness of these safeguards;
- Select and retain service providers that are capable of maintaining appropriate safeguards for the information and require them, by contract, to implement and maintain such safeguards; and
- Adjust the information security program in light of developments that may materially affect the program. [1]

completely erase all confidential data
user-selectable erasure patterns

Are You in Compliance?

How do you stay in compliance when you perform a Disaster Recovery test at an unsecured, third-party hot site location?

SAE & Fast DASD Erase

In the past, many organizations simply clipped the VTOC at the end of their Disaster Recovery tests at a Hot Site. But erasing test data at the end of a Disaster Recovery test may be one of the most important steps of the test itself. Your data (and its security) is your responsibility; it is not the responsibility of the hot site vendor. Stand Alone Environment (SAE) users enjoy peace of mind knowing they have completely erased all confidential data, thereby safeguarding it from unwanted use. It is also invaluable when decommissioning DASD. The Fast DASD Erase tool not only clips the VTOC; it completely destroys all data.

Government regulations and internal procedures may call for multiple erasure passes. SAE provides user-selectable erasure patterns, allowing users to write a random byte value in addition to binary zeroes across tracks during Fast DASD Erase.

Stand Alone Environment is available for FREE, 30-day trials. It can be downloaded from the NewEra website -- www.newera.com.

Download today at www.newera.com

Sources
[1] http://www.ftc.gov
[2] http://www.ftc.gov/privacy/glbact

NEWERA
Standards for OS/390 System Management

Corporate Headquarters
Morgan Hill, California 95037
800 421-5035
TEL: 408-201-7000
FAX: 408-201-7099
email: info@newera.com