

Information Security Compliance in the Internet Age

Measuring up with the GLBA

Measuring Up with the GLBA

The Gramm-Leach-Bliley Act (GLBA) dictates that Financial Institutions must protect customer information, as well as delineates jurisdiction for regulatory agencies. Most community banks fall under the authority of the FDIC, which publishes guidelines and administers examinations. As the security threat environment evolves, the FDIC continually updates their recommendations and examination procedures.

What Does The Gramm-Leach-Bliley Act Actually Say ?

As we all know, Banking is a much regulated industry, with most regulations resulting from acts of Congress. As far as securing customer information is concerned, the GLBA, specifically section 501(b), defines the intent of the government. Although this section is only 95 words, its impact on Financial Institutions has been tremendous:

Section b – Financial Institutions Safeguards – in furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards –

(1) – To insure the security and confidentiality of customer records and information;
(2) – to protect against any anticipated threats or hazards to the security or integrity of such records;

and

(3) – to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

The policy referenced in the first sentence states that Congress believes that FI's have an obligation to protect customer data. Section 505(a) delineates who has authority over various types of FI's. The FDIC is the authoritative agency for those banks it insures, other than those who are members of the Federal Reserve System, or those that fall under the Office of Thrift Supervision.

What FDIC Standards Are Used to Measure Compliance With The GLBA ?

The FDIC publishes guidelines and standards for securing customer information through its 'Financial Institution Letter' publications, and has developed FI examination procedures which measure the institutions' abilities to satisfy GLBA mandates. There are three examinations used by the FDIC, presented here in increasing order of comprehensiveness:

- IT-MERIT Procedures (**M**aximum **E**fficiency, **R**isk-focused, **I**nstitution **T**argeted)
www.fdic.gov/news/news/financial/2002/fil11802b.html
- IT General Work Program
www.fdic.gov/new/news/financial/2002/fil11802a.html#4-1
- Federal Financial Institutions Examination Council (FFIEC) Work Programs.
www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

Which Examination Applies to My Bank ?

To determine which examination should be applied, FI's are classified into one of four technology risk profiles. The classifications are not based upon asset size, but rather the extent of technology risk they represent. The non-public profiling methodology is based on characteristics such as extent of E-Banking offerings, degree of outsourcing of services, core banking and vendor management

risk areas and others. Many community banks are categorized as Type I institutions, for which the IT-MERIT Procedures apply. Type II institutions will require the IT General Work Program to be utilized, while Type III and IV are associated with the IT General Work Program plus some or all of the FFIEC Work Programs. The difference between type I and II institutions is ‘a History of less than satisfactory examination ratings’¹. Being prepared for an IT-MERIT examination is key to maintaining a satisfactory history. Understanding the examination procedures and the areas of focus within them are the foundations of being prepared.

What Happens When We Don’t Pass With Shining Colors ?

According to Marlene Roberts - Examination Specialist (IT) for the San Francisco Region of the FDIC – when there are findings that require remediation, if they are deemed not to be serious issues, the FDIC will revisit these items in the next scheduled exam (12-18 months). For more serious security problems, the FDIC may require a letter of acknowledgement from the FI’s board of directors (which ties in with the Sarbanes-Oxley Act) relating to the issues. The FI will have a scheduled ‘visitation’ by FDIC examiners 6 months later, which will focus on the findings and the progress of their remediation. If all goes well, the FI will have a subsequent examination 12-18 months after the previous full examination.

What’s Coming ?

In a word - Change. The information security threat environment is evolving at a high rate. Exploits and attacks that required highly skilled experts a year ago are now freely available scripts that almost anyone with an internet connection can use to threaten financial institutions. Banking regulatory agencies are adapting to the changing environment with frequent publishing of guidelines and recommendations, backed up with examinations. Examinations and Work Programs are constantly being updated, and as long as FI’s understand the continuous need for improvement of IT security, the partnership between them and the regulatory agencies will result in a more secure national financial system.

¹Source: ‘The FDIC’s Progress in Implementing the Gramm-Leach-Bliley Act, Title V – Privacy Provisions’, Audit Report No. 03-044 dated September 26, 2003
www.fdic.gov/oig/a-rep03/03-044-508.html