

## GLBA Compliance: How to Avoid Common Traps

The Financial Modernization Act of 1999, AKA the Gramm-Leach-Bliley Act, or just plain GLBA.

However you know it, financial institutions now have had several years of regulatory oversight and examination on it, but some are still struggling to meet the regulation's myriad list of requirements, which include provisions to protect consumers' personal financial information held by financial institutions.

Specific components of GLBA include The Safeguards Rule, which requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule mandates that financial institutions develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information.

The plan should include:

- Denote at least one employee to manage the safeguards;
- Construct a thorough risk assessment on each department handling the nonpublic information;
- Develop, monitor and test a program to secure the information;
- Change safeguards as needed with the changes in how information is collected, stored and used.

This rule is intended to ensure what financial institutions already should be doing - protecting their clients' information. It makes financial institutions take a closer look at how they manage private data and to do a risk analysis on their current processes.

How do you know if your institution is on the right track toward GLBA compliance? The most obvious signs of a strong compliance program begin with defined roles and responsibilities. Is your compliance a **"top-down strategy that is connected directly to the Board of Directors?"** The existence of a primary compliance person in charge of the many required activities is another marker. Having an Information Security Officer (ISO) working on core compliance activities is another key compliance marker.

- How comprehensive and available are key policy/procedure documents (primary is the Information Security Policy)?
- Does the documentation reflect accurately on the institution and its culture, or is it a stand-alone artifact use only to try and ward off examiners and auditors?
- Is there a thorough risk assessment available, and was it conducted recently?
- Are current compliance activities aligned against the risk assessment?
- How solid is the vendor management program and is it maintained?
- Is there a BCP that includes the entire institutions (not just IT), and was it designed and/or updated to address a recent business impact analysis?
- Is there an Incident Response plan that staff has been trained to use?
- Have any of the core programs/procedures been properly tested?

Signs of an institution that may be at risk are incomplete or wrong answers to any of these questions. Not knowing who is responsible for the core compliance activities is almost always an indicator that there are issues present. Incomplete, outdated or missing documentation is also a concern. Procedures that have either never been validated or haven't been tested recently are problem indicators as well. When there are very obvious issues, such as improperly designed IT architecture or poor physical security, it's rare that those are isolated problems.

*Be sure to keep an eye out for future installments which will showcase GLBA compliance elements such as Board of Director education, Information Security programs, GLBA privacy decisions, Incident response plans, and vendor management programs.*

*Source: July 7, 2008 - Linda McGlasson, Managing Editor  
www.bankinfosecurity.com*

## LESSONS LEARNED FROM HURRICANE KATRINA: Preparing Your Institution for a Catastrophic Event

### Part IV

For the past three months, we have featured a piece on some important disaster recovery lessons learned following the aftermath of Hurricane Katrina. This month, we bring you final installment of the series.

- **Lesson Learned – The financial industry is dependent on numerous critical infrastructure sectors that potentially have competing interests.**
  - You may want to contact local and state officials to understand the priority that will be given to financial institutions to restore critical services. You can reach your state homeland security contact at [www.DHS.gov/dhspublic/display?theme=11&colIntent=3138](http://www.DHS.gov/dhspublic/display?theme=11&colIntent=3138).
- **Lesson Learned – A financial institution's involvement in neighborhood, city, state, federal, and nonprofit or volunteer programs can facilitate a community's recovery from a catastrophic event.**
  - You may want to contact local chapters of nongovernmental organizations, such as non-profit, volunteer, and private sector entities, to discuss ways the organizations might work together to benefit the community.
  - You may want to maintain a list of regulatory points of contact and reference data to establish clear lines of communication between your institution and primary regulator.

#### State and Federal Regulatory Agencies

**Florida Office of Financial Regulation**  
[www.flofr.com/banking/index.htm](http://www.flofr.com/banking/index.htm)  
(850) 410-9800

**Alabama State Banking Department**  
[www.banking.alabama.gov](http://www.banking.alabama.gov)  
(334) 242-3452

**Georgia Department of Banking & Finance**  
<http://www.ganet.org/dbf/dbf.html>  
(770) 986-1633

**California Dept of Financial Institutions**  
[www.dfi.ca.gov](http://www.dfi.ca.gov)  
(415) 263-8555

**North Carolina Banking Commission**  
[www.nccob.org/NCCOB](http://www.nccob.org/NCCOB)  
(919) 733-3016

**South Carolina State Board of Financial Institutions**  
[www.state.sc.us/treas/financial\\_board/board.html](http://www.state.sc.us/treas/financial_board/board.html)  
(803) 734-2001

**Tennessee Department of Financial Institutions**  
[www.tennessee.gov/tdfi](http://www.tennessee.gov/tdfi)  
(615) 741-2236

**Virgin Islands Division of Banking and Insurance**  
(340) 774-7166

**Federal Financial Institutions Examination Council**  
[www.FFIEC.gov](http://www.FFIEC.gov)

**Federal Deposit Insurance Corporation**  
[www.FDIC.gov](http://www.FDIC.gov)  
(877) ask FDIC or (877) 275-3343

**Federal Reserve System**  
[www.FederalReserve.gov](http://www.FederalReserve.gov)  
(202) 452-3000

**National Credit Union Administration**  
[www.NCUA.gov](http://www.NCUA.gov)  
(703) 518-6300

**Office of the Comptroller of the Currency**  
[www.occ.treas.gov](http://www.occ.treas.gov)  
(202) 874-4700

**Office of Thrift Supervision**  
[www.ots.treas.gov](http://www.ots.treas.gov)  
(800) 958-0655 or (202) 906-6000



Source: FFIEC

## The Get-Away-From-it-All Checklist

It's summertime, your bags are packed and you're ready to go!...Or so you think. Did you turn off the oven? Did you tell the post office to hold your mail? **Did you set your OOF?** If you said "yes" to the first two but are scratching your head about that last one, this is for you. When you're preparing to go on vacation, it's best to take care of some things at the office before you leave. That way, when you return, you won't have an angry pile of e-mail messages in your inbox or a line of people waiting outside your office.

If your company is running Outlook with Exchange Server, you can use a handy feature called the **Out of Office Assistant**. This feature lets you create a reply message to e-mail sent to you while you're away. It also lets you set up specific rules about who to reply to, how often, even how to file the messages.

Whether you use the Out of Office Assistant or set up a rule, when you create your message (affectionately known as your OOF, for "Out of Office") consider mentioning that you're gone, noting when you'll be returning, and giving the sender another person to contact in your absence. If you leave an alternate e-mail address or number that could be used to track you down while you're away, keep in mind that you'll be fair game for work-related calls while you're enjoying your vacation.

If you use Outlook with Exchange at work, you'll want to **mark your Outlook calendar to reflect that you are out of the office**. That way, if someone tries to schedule you for a meeting, they'll see that you're gone and not available.

If you've got recurring meetings that will happen while you're out, the courteous thing to do is **decline those meetings**. It's also nice to let the organizers know why so that it doesn't seem as if you're gratuitously shooting back a "No! I'm not coming!" If you're the organizer, **send out a cancellation**.

### *A few more things to think about:*

- ✓ *Don't leave your cell phone number on your whiteboard.*
- ✓ *Change your outgoing voicemail message.*
- ✓ *Turn off your computer.*
- ✓ *Check the oil in the car.*
- ✓ *Make sure your airline hasn't gone out of business.*
- ✓ *Turn off the lights.*
- ✓ *Don't forget to write!*



*"Vacation is what you take when you can't take what you've been taking any longer."  
Cowardly Lion (Wizard of Oz)*

*Source: Annik Stahl, the Crabby Office Lady columnist*

*Are there topics that you would like to have covered in future newsletters? We are always looking for topics of interest. We welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please email Shama Renée-McIntosh at [smcintosh@aaSysgroup.com](mailto:smcintosh@aaSysgroup.com).*