



11301 NORTH US HIGHWAY 301, SUITE 106
THONOTOSASSA, FL 33592
(813) 246-4757 • (813) 246-4576 (FAX)
WWW.AASYSGROUP.COM

ISSUE 2

VOL 6

FEB 2008

Solutions

are our business

Risk Management Agenda

Top 10 Challenges that Financial Institutions Face

If 2007 is any indication, then 2008 is going to be a wild year for financial institutions facing a slew of risk management issues.

Financial institutions, regulators, banking service providers, industry associations and information security experts - they all voice similar concerns about the top information security challenges facing the industry in 2008. Following is a list of the Top 10 risk management challenges.

1) Keeping up with Compliance

Historically, the Credit Union National Association finds that only about 10 percent of credit unions have a person dedicated primarily to compliance. The others generally rely on a senior officer to handle this area - on top of other, non-security responsibilities. Security, therefore, is put on the back burner, causing companies to miss things that may make them vulnerable to attack from both inside and outside of the company. The same, of course, is true at small banks.

There is no shortage of new regulatory requirements coming down the pike. If your institution cannot keep up with the flow now, then it's time to either dedicate or expand your available resources. Non-compliance is not an option.

2) New Regulations

And if your current regulatory requirements aren't enough, expect to see more in 2008 (see page 2 for a list of some of 2008's new regulatory requirements). Whether your institution is working toward compliance on ID Theft Red Flags or the recently released FFIEC Pandemic Guidance, "Make sure your risk assessments are current and up-to-date," says FDIC spokesperson David Barr.

3) Insider Threat

This is something that financial institutions fear the most -- a trusted insider who either intentionally or unintentionally leaks data out of the institution. The causes range from malicious employees bent on removing information to the unintentional employee's mistake of falling prey to a social engineering attempt. Also placing the

institution at risk is outsourced business operations. Information security experts point to institutions that don't have proper protection then put themselves at risk from the data center, the help desk, the supply chain, vendors and contractors. Increasing incidents of fraud, theft and insider threat may arise from outsourcers who may lack accountability, loyalty, or security policy implementation.

4) Identity Theft

With the estimated number of identity theft victims rising and marching orders given in the ID Theft Red Flags guidance issued in late 2007, the entire industry must answer how institutions are protecting their customers' information. Institutions must answer how they are educating their employees and customers, as well as how to create better mechanisms to verify new account openings, especially in the online environment. Institutions also need to work closely with local law enforcement. One solution strongly suggested is by regulators and the ID Theft task force is to reduce the use of social security numbers as identifiers for customer accounts.

5) Data Breaches Caused by Human Error

The unaware employee, consultant, contractor or third party service provider staffer is an institution's worst enemy. To avoid becoming the industry's version of a TJX-level data breach, institutions need to develop corporate policies that protect the organization from employees' electronic behavior occurring outside the corporate perimeter.

6) Business Continuity -- Pandemic Planning

Institutions can expect that their regulators will ask about their pandemic plan and will want to see it as part of an overall BCP/DR plan for the institution. Elements to include in your institution's pandemic plan include a preventive program to reduce the pandemic's impact on operations; a comprehensive framework of facilities, systems and procedures to continue critical operations if large numbers of staff are unavailable for extended periods; testing of the plan and oversight to ensure timely updates; and

ongoing review of the institution's pandemic plan.

7) PCI Compliance; Debit Card Fraud Prevention

Complying with the 'digital dozen,' or the Payment Card Industry's 12 requirements for data protection, is a challenge for most financial institutions. Compliance with the PCI Data Security Standards means that your institution is better prepared to protect not only credit card data, but the rest of your institution's information.

8) Employee and Customer Awareness

Institutions need to better educate their employees and customers about the security threats that are facing them and their customers. Now with the ID Theft Red Flags, it's also been pushed to the top of the compliance list. Institutions by Nov. 1 must have a written program showing how they are educating their employees and customers about identity theft.

9) Criminal Attacks

With the increased number of online attacks against financial institutions in 2007, including more sophisticated phishing and other types of criminal attacks aimed at both institutions and their customers, the coming year looks to be more of the same. In addition to traditional phishing attacks, institutions also need to prepare for malware-based attacks. This type of attack distributes malicious content to unsuspecting users through Web site visits and nefarious downloads.

10) Managing Third-Party Risk

The FDIC sees vendor management as a trend important enough to include in its updated IT Risk Management Program Examination Procedures questionnaire in December 2007. Other banking industry regulators are also expected to look more closely at how their regulated institutions are managing their third-party service providers, and how strenuously they are examining the vendor's information security program and data protection strategies.

NEW REGULATORY REQUIREMENTS TO LOOK OUT FOR IN 2008

Below is a list of some new Regulatory Requirements that may be issued in 2008:

- **ID Theft Red Flags** - These final rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. Under these new rules, which take effect Jan. 1, 2008, each financial institution's Identity Theft Prevention Program must include: reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable the financial institution to identify relevant patterns, practices, and specific forms of activity that are 'red flags' signaling possible identity theft and incorporate those red flags into the institution's program. Deadline for compliance is Nov. 1, 2008.
- **New FFIEC Requirements** - update to the IT Examiners Handbook is expected sometime in 2008
- **FFIEC Pandemic guidance** - This guidance expands upon the contents of the Interagency Advisory on Influenza Pandemic Preparedness issued in March 2006. Accordingly, an institution's business continuity plan should include:
 - ✓ A preventive program to reduce the likelihood an institution's operation will be significantly affected by a pandemic event;
 - ✓ A documented strategy that provides for scaling pandemic efforts commensurate with the particular stages of a pandemic outbreak;
 - ✓ A comprehensive framework of facilities, systems, or procedures to continue critical operations if large numbers of staff members are unavailable for prolonged periods;
 - ✓ A testing program to ensure the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue; and
 - ✓ An oversight program to ensure ongoing review and updates to the pandemic plan.

- **FDIC IT Risk Management Program amendments** - the new IT exam questionnaire is out, and it deals with new issues such as vendor management. You can only expect other regulators to follow suit with new requirements.
- **Anti-Money Laundering** - the Bank Secrecy Act examination manual was revised in 2007, and there's every reason to expect new requirements in 2008.
- **BASEL II** -As banking institutions do more business internationally, then increasingly they must meet these recommended global banking standards.

AaSys to Launch New Intranet Site Service

AaSys will be introducing a new service which will allow our Banking Customers to launch new **Intranet Sites**. This service is a turn-key intranet solution designed for community banks and will provide a company-wide portal solution giving every member of your organization all the information they need with a click of a mouse.

This new service uses an easy, secure administrative module for content providers that ensure the intranet experience always starts with fresh and up-to-date information.

Contact AaSys for more information!



Announcements.....!

AaSys Group will be closed on Monday, February 18th in observance of President's Day.

In the event that we need to contact you in an emergency and your business lines are down, **please forward us your alternate emergency contact phone numbers.**

Please forward all phone numbers to smcintosh@aasysgroup.com.

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.