



ISSUE 4

VOL 6

APR 2008

# Solutions

## are our business

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

## Is Your Disaster Recovery Plan Up to Date?

Disaster Recovery is the process, policies and procedures of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (incoming, outgoing, toll-free, fax, etc.), workspace, and other business processes after a natural or human-induced disaster.

To increase the opportunity for a successful recovery of valuable records, a well-established and thoroughly tested disaster recovery plan must be developed.

***Hurricane Season is almost upon us. Is your Disaster Recovery Plan up to date? Has it been reviewed and tested? Now is the time to evaluate your procedures!***

Contact your AaSys Account Manager now for more information on Disaster Recovery Planning and Business Continuity!



## Pandemic Progress Report - How Do You Rate?

When it comes to pandemic preparation at U.S. financial institutions, it's a case of good news/bad news.

Bad news first: Many mid-sized and smaller financial institutions are not fully compliant with the recent FFIEC pandemic guidance and don't have formalized pandemic preparedness plans yet in place.

But the good news: several financial institutions, as a result of regulatory pressure, are working toward having a completed pandemic plan in place as part of their overall Business Continuity Plan (BCP).

If your plan is out of date, or if you don't have a plan in place yet, please contact your AaSys Account Manager for more details.

### **New Business Continuity Guidance Issued by FFIEC Revised Booklet Stresses Business Impact Analysis, Pandemic Planning**

The FFIEC issued long-awaited new guidance on business continuity planning. The update - the first in five years - includes increased focus on business impact analysis and testing, as well as new emphasis on pandemic planning.

This new booklet is aimed at examiners, financial institutions and technology service providers to identify business continuity risks and evaluate controls and risk management practices for effective business continuity planning. This guidance updates the "**Business Continuity Planning Booklet**," issued in March 2003. For your copy, type the following URL into your browser: [http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus\\_continuity\\_plan.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf)

Source: [www.bankinfosecurity.com](http://www.bankinfosecurity.com). March 21, 2008, Linda McGlasson

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



## Part I

Financial institutions have responded admirably to the unique challenges raised by successive hurricane seasons with significant storms. Business continuity plans generally worked very well in enabling institutions to meet these challenges and to restore operations swiftly. However, the unprecedented magnitude and duration of the effects of Hurricane Katrina caused major disruptions that exceeded the scope of the disaster recovery and business continuity plans of some financial institutions. Many institutions had to adjust plans and improvise responses to successfully address unexpected complications. Overall, institutions prevailed in very difficult circumstances through advance planning and preparation, and by working together. As a result of these efforts, the financial industry was able to assist customers and communities in their time of greatest need. You may want to consider this information when conducting a review of your institution's disaster recovery and business continuity plans. ***These lessons learned should not be construed as new regulatory requirements, nor do they supplant or modify the guidance provided by the FFIEC in its Business Continuity Planning Booklet.***

- **Lesson Learned – Some organizations may not have anticipated or prepared for the extensive destruction and prolonged recovery period resulting from Hurricane Katrina.**
  - You may want to reassess how well your institution is prepared for reasonably foreseeable threats across all levels of the organization, not just from the perspective of recovering your information technology.
  - Developing, implementing, and regularly testing disaster recovery and business continuity plans to ensure their continued effectiveness for responding to changing business and operational needs is key.
  
- **Lesson Learned – To be realistic, disaster drills should include all critical functions and areas.**
  - Disaster drills should be relevant to a specific location (considering infrastructure, population centers, weather, threats of terrorism, natural disasters, etc.) and include worst-case scenarios.
  - After conducting a drill, you should review the results to determine what worked correctly, what went wrong or not as expected, what areas can be improved, and what, if any, adjustments to your plans are needed.
  - Employees at every level of your organization should know their role in the disaster recovery and business continuity plans.
  
- **Lesson Learned – Anticipate disruptions in communications services, possibly for extended periods of time.**
  - You may want to develop, test, and update a contact list for senior management, employees, customers, vendors, and key government agencies. Maintaining copies of this information at all sites, plus one or more off-site locations, can be very helpful in the event of a disaster.
  - You may want to establish a central point of contact outside the potential disaster area and make pre-established toll free telephone numbers available for employees and customers.
  
- **Lesson Learned – Critical staff may not be able to reach their assigned recovery location.**
  - You may want to identify alternative, prioritized gathering place(s) for employees to meet after a disaster.
  - You may want to consider what type(s) of credentials employees will need to gain access into a disaster area, as authorities may restrict re-entry.

***Be sure to look out for Part II in the May 2008 issue!***



Source: FFIEC

## AASYS PARTNERS WITH ONECOMPLY FOR GLBA RISK ASSESSMENTS

AaSys has contracted with SourceSentry in utilizing their OneComply web based solution for conducting all GLBA Operational Risk Assessments. The application and the results will be hosted on a secure server hosted at AaSys and the Bank will receive a one year license for use of OneComply. A portal requiring a user name and password will be established and an SSL connection will further secure access to the application.

OneComply is a tool that allows financial institutions to assess compliance, track activities and measure internal controls. Using the framework provided by OneComply, an organization's focus moves away from when and how to complete an assessment, and instead focuses on the remediation of identified risks. OneComply provides for consistent standards to be applied throughout all phases of the organization's processes.

The flexibility of OneComply allows a financial institution to define the scope of a risk assessment, and this scope can be increased or decreased, depending upon the need of an organization. For instance, an organization may choose to assess various departments on a monthly basis, or to assess different locations on a quarterly basis.

OneComply ensures that all compliance documentation be kept in a central location. This facilitates the audit process.

OneComply can be used across the entire organization, with different individuals allowed to assess their individual areas. Rights are assigned to individuals as follows:

- Administrator
- Assessor
- Read-Only Viewer
- Report Viewer

This process enhances security and allows compliance activities to be delegated across roles. OneComply also tracks work flow and email notifications enable communication throughout the risk assessment process.

Finally, OneComply provides for trend analysis. It is possible to create reports detailing the progress an organization has made over a defined span of time.

For more information, contact your AaSys Account Manager.

## EXTRA! EXTRA!

Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats allows users to open, edit, and save documents, workbooks, and presentations in the file formats new to Microsoft Office Word, Excel, and PowerPoint 2007. The Compatibility Pack can also be used in conjunction with the Microsoft Office Word Viewer 2003, Excel Viewer 2003, and PowerPoint Viewer 2003 to view files saved in these new formats. For more information about the Compatibility Pack, please copy and paste the following link into your browser:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=941b3470-3ae9-4aee-8f43-c6bb74cd1466&displaylang=en>.

Customers who purchased Office 2003 with a new computer will continue to receive support for the 2003 release products based on their OEM's or System Builder's policy. Customers who purchased Office 2003 from a reseller will have access to Mainstream Support until January 13, 2009. This means retail customers can place calls to Microsoft Customer Service and Support about Office 2003-related issues for the following:

- *Incident support (no-charge incident support, paid incident support, support charged on an hourly basis)*
- *Security update support*
- *The ability to request non-security Hot Fixes*



## Congratulations!

**Jamil Porta**, AaSys Service Engineer, recently acquired an Associates of Science Degree in Computer Network Engineering. Jamil already has a Bachelors of Science in Computer Science with a minor in Mathematics and he is also a Microsoft Certified Professional. Currently, he is working on obtaining his Microsoft Certified Systems Administrator Certification.

**Adrienne DiTunno** and **Kofi Kankam**, AaSys Help Desk Engineers, who previously held certifications in MCSA 2000 (Microsoft Certified Systems Administrator) and MCSE 2000 (Microsoft Certified Systems Engineer) recently passed their 2003 exams and now hold certifications in MCSA 2003 and MCSE 2003.

*Please join AaSys in welcoming the following individuals to our stellar Team:*  
**Elizabeth Patrick, Field Service Engineer / IT Consultant**  
**Susan Hubbard, Account Manager**