

Why business continuity makes good business sense

The September 11th terrorist attacks...hurricanes Katrina and Rita... Avian flu pandemic predictions. The beginning of the 21st century has already provided plenty of reasons to take emergency planning seriously. Be it terrorism, extreme weather or potential pandemic illness, financial services providers are acutely aware that events out of our control may wreak havoc on our operations.

The big picture: Interdependency

The terrorist attacks of September 11, 2001, made it clear that financial institutions are interdependent in many ways. In a speech before the Institute of International Bankers just six months after the attacks, the Federal Reserve Board of Governors' vice chairman at the time, Roger W. Ferguson, said:

Most important, we learned, as a result of these interdependencies, that contingency-planning decisions made by an individual institution may affect not only the safety and soundness of that institution, but also the safety and soundness of other institutions and, indeed, the very functioning of the financial markets. As a result, we believe that coordinated discussions of sound practices for business continuity involving the financial industry and regulators are an important part of our response to the events of September 11.¹

For the benefit of the nation's banking system overall, financial institutions must do their part to be prepared. In fact, regulatory agencies require it. "Because financial institutions play a crucial role in the United States economy, it is important their business operations are resilient and the effects of disruptions in services are minimized in order to maintain public trust and

confidence in our financial system," states the Federal Financial Institutions Examination Council (FFIEC) *Business Continuity Planning* booklet. This booklet serves as a reference for the institutions overseen by the:

- Federal Reserve Banks
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Office of Thrift Supervision (OTS)

The FFIEC maintains other business continuity resources at www.ffiec.gov, including, "Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event." This report lists specific actions to take in the event of a natural disaster that may trigger a run on cash.

Many of the regulatory Web resources make it clear that business continuity is a matter of managing risk and keeping the public trust. Bank examiners, auditors, investors and the general public expect it. With this in mind, the BITS Financial Services Roundtable, a non-profit industry consortium whose members include 100 of the largest U.S. financial institutions, maintains a crisis management Web site, www.bitsinfo.org. From the *Publications* link, you can explore materials categorized under topics that include crisis management coordination, fraud reduction and operational risk.

¹ Source: "A Supervisory Perspective on Disaster Recovery and Business Continuity" by then Vice Chairman Roger W. Ferguson, Jr., before the Institute of International Bankers in Washington, D.C. on March 4, 2002.

Tying in public health, telecommunications, electricity and financial infrastructure, the information on the BITS Web site highlights the significance of business contingency given the interdependence of the players in the nation's economic infrastructure.

The Federal Reserve Banks stand ready

The Federal Reserve Banks are committed to continuing operations during emergency situations. Of course, this is not a guarantee that there will never be a service disruption due to an unforeseen catastrophic event, but it is a pledge that the Federal Reserve Banks strive to provide the best support possible, in any scenario, and maintain open lines of communication, at all times.

To help safeguard the nation's financial infrastructure, the Federal Reserve Banks maintain business continuity plans to address possible threats to our operations. These plans are tested and updated on an ongoing basis by every service area and by each Federal Reserve District.

Specifically, critical transaction services, including the Fedwire Funds Service, Fedwire Securities Service and FedACH Services, as well as Account Services and other information services accessed via the FedLine access solutions, have undertaken rigorous contingency planning and testing to help ensure resiliency. Similarly, financial institutions should review contingency plans, check periodically for updates and keep hard copies for reference (in case of power loss or relocation).

The Federal Reserve Banks' *National Business Continuity Guide*, available online at www.frb services.org/BizContinuity/, contains materials to help prepare for a potentially disruptive emergency. The online guide contains links to service-specific continuity plans. The *Cash Services Guide*, for example, contains a "Checklist for Fed-Related Preparations" to help prepare cash operations employees for the possibility of a business disruption.

Another valuable online tool—*My FedDirectory*—generates a customized list of Federal Reserve Bank contacts that can be printed and saved as a reference in case an emergency cuts off your Internet access.

For more information

Taking a proactive approach to business continuity planning makes good business sense for the financial services industry. If you have questions regarding business continuity planning, contact your account executive via *My FedDirectory* on www.frb services.org.

FS-ISAC Center helps to safeguard U.S. from physical and cyber security threats

To help protect the U.S. critical infrastructure, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was established to facilitate information sharing between the public and private sectors about physical and cyber security threats and vulnerabilities.

Created in 1998 as a result of Presidential Decision Directive 63 (PDD-63), then updated in 2003 with Homeland Security Presidential Directive 7 (HSPD-7), the FS-ISAC is a nonprofit private sector initiative designed and developed to provide a single, accurate and timely source for sharing physical and cyber security information.

The mission of the FS-ISAC, in collaboration with the U.S. Department of the Treasury and the Financial Services Sector Coordinating Council, is to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents, and to serve as the primary communications channel for the sector.

Bill Nelson, FS-ISAC president & CEO, said, "The FS-ISAC has been providing tremendous value to the financial services sector and its 4,000 members. In particular, members receive a direct return on their investment that is as high as 1900:1. This is achieved through the maintenance of a 24/7 security operations center that facilitates the exchange of information and with accurate and timely analysis of cyber threats, vulnerabilities and incidents that the members cannot obtain elsewhere."

For more information about FS-ISAC, including how to join and membership benefits, visit www.fsisac.com.