



**COMPUSHARE**

**Compass**  
financial direction you can count on

# New Business Continuity Guidance Issued by FFIEC: Build an Enterprise-Wide Business Continuity/ Disaster Recovery Program

By Debbie Payne, CBCP

Business Continuity Specialist, Risk & Compliance Compushare, Inc.

Over the last few years there has been a strong focus on the need to develop an Enterprise-Wide Business Continuity Program in both industry and government. All sorts of events have triggered this ranging from 9/11 and other terrorist events, to climatic events and regulatory pressures. Ensuring that an institution's assets, operations, commitments and relationships are protected enterprise-wide is a critical element of staying in business. The frequency and severity with which isolated and regional disasters are occurring today prove that planning for the recovery phase of Information Technology alone is simply not enough.

On March 19, 2008, the Federal Financial Institutions Examination Council (FFIEC) Task Force on Supervision issued updated guidance for examiners, financial institutions, and technology service providers to identify business continuity risks and evaluate controls and risk management practices for effective business continuity planning. The guidance is an update to the "Business Continuity Planning Booklet," which was issued in March 2003.

The revised booklet includes enhancements to the business impact analysis and testing discussions, and addresses emerging threats and lessons learned in recent years. The booklet also stresses the responsibilities of each institution's board and management to address business continuity planning with an "enterprise-wide" perspective by considering technology, business operations, communications, and testing strategies for the entire institution. While many banks and credit unions have some form of a business continuity plan in place since the 1970s, few plans encompass all of the risks that now face financial institutions today. In the past, contingency planning was thought to be necessary for only information systems-related activities. Business recovery has moved beyond recovering computer systems to restoring and recreating business processes. The outage of whole departments must be considered, and how work and information will flow from one place to another. A successful enterprise-wide Business Continuity/Disaster Recovery program will move beyond the IT department and into the business area of the organization to include:

- Soliciting commitment from the Board of Directors and Top Management. If senior management is not committed to the process, chances for success are poor
- Performing Risk Assessment and Business Impact Analysis. This initial assessment should define the institution's needs in an emergency and provide information on the requirements for the alternate site. This is an important function in the planning process as it will provide a firm foundation for the development of an effective plan. A business impact analysis determines what needs to be recovered and how quickly it needs to be recovered.
- Prioritizing recovery needs and interdependencies.
- Developing Business Continuity

Strategies.

- Developing and implementing the plan.
- Testing the plan. Testing is an extremely important part of the business continuity program. Testing should be addressed with an enterprise-wide perspective by considering technology, business operations, communications and strategies for the entire institution. Only when a plan is rehearsed will any weaknesses be revealed, and you will be able to prove to the board that in the event of a disaster your institution can cope.
- Continuous testing and evaluation of the plan.

Key elements of the FFIEC's "December 2007 Interagency Statement on Pandemic Planning" have been added to the booklet. A pandemic outbreak would present unique business continuity challenges. The methodologies detailed in the booklet provide a framework for financial institutions to develop or update their pandemic preparedness plans. All financial institutions should have plans that address how the institution will function during a pandemic event including:

- A preventive program to reduce the likelihood that an institution's operations 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 of time.
- A testing program to ensure that the institution's pandemic planning practices and capabilities are effective and will



allow critical operations to continue.

- An oversight program to ensure ongoing review and updates to the pandemic plan.

Other changes in the booklet highlight the importance of business continuity planning for all financial institutions, regardless of size or whether their systems are provided in-house or through third-party service providers, as well as lessons learned from financial institutions that suffered damage from hurricanes Katrina and Rita. Plans should take into consideration any outsourced functions. Many banks outsource data processing or specialized applications such as trust accounting, credit card operations, and automated teller machine applications. These functions must be defined and addressed in a Business Continuity/Disaster Recovery plan.

### **Conclusion**

The updated guidance should serve as a wake-up call for banks and credit unions that have not done enough to meet their Business Continuity Planning requirements. Changes in business processes and technology, increased terrorism concerns, recent natural disasters and the threat of a pandemic have all focused attention on the need for Business Continuity Planning. The key to successful Business Continuity/Disaster Recovery Planning is what happens long before a disaster strikes. Only a realistic enterprise-wide Business Continuity/Disaster Recovery Program, properly implemented, tested, maintained and committed to by senior management, will deliver maximum business resilience and all the benefits that a financial institution should rightly be seeking. It is painstaking work, but it will make the difference between continued success and business failure.