

## **Federal Financial Regulators Release New BCP Booklet**

On May 20, 2003, the Federal Financial Institutions Examination Council (FFIEC) issued revised guidance for examiners and financial institutions to use in evaluating risk-management processes to ensure the availability of critical financial services. This guidance – *The Business Continuity Planning Booklet* – is the second in a series of updates to the 1996 *FFIEC Information Systems Examination Handbook*.

The FFIEC agencies plan to distribute these books electronically via the Internet through the FFIEC's InfoBase application. The InfoBase includes each booklet in Adobe Acrobat file format as well as an online version with links to various resource materials and an orientation to the handbook update process. The new documentation can be found at:

<http://www.ffiec.gov/guides.htm/htm>

Over the next few months *Vision Views* Information Security Focus will summarize and discuss portions of the new Business Continuity Planning Guidelines.

### **Introduction**

Operating disruptions can occur with or without warning, and the results may be predictable or unknown. Financial institutions play a crucial role in the country's economy, and in the day-to-day business activities of their customers. Accordingly it is crucial that bank business operations are resilient and the effects of disruptions in service are minimized in order to maintain public trust and confidence in the financial system. Effective business continuity planning establishes the basis for financial institutions to maintain and recover business processes when unexpected disruptions of operations occur.

Business continuity planning is the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants; and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations. Changing business processes (internally to the institution and externally among interdependent financial services companies) and new threat scenarios require financial institutions to maintain updated and viable BCPs.

### **BCP Booklet Contents**

The FFIEC Business Continuity Planning booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes established to ensure the availability of critical financial services. Major sections of the booklet include:

- Introduction
- Board and Senior Management Responsibilities
- Business Continuity Planning Process
  - Business Impact Analysis
  - Risk Assessment
  - Risk Management

- Other Policies, Standards and Processes
- Risk Monitoring
- Summary
- Appendix A: Examination Procedures
- Appendix B: Glossary
- Appendix C: Internal and External Threats
- Appendix D: Interdependencies
- Appendix E: BCP Components

Reviewing BCPs has long been a major component of the examination process. However, new business practices, changes in technology, and increased terrorism concerns have focused even greater attention on the need for effective business continuity planning, and have altered the benchmarks for measuring plan effectiveness. For example, today's effective BCP should take into account the potential for wide-area disasters with impact on an entire region with a resulting loss or inaccessibility of staff. It should also consider and address market-based and geographic interdependencies among financial system participants as well as infrastructure service providers. In most cases, recovery time objectives are now much shorter than they were even a few years ago, and for some institutions, applications and service providers, recovery time objectives may be measured in hours or even minutes.

### **Next Month – Board and Senior Management Responsibilities**

Stephen Tonn is the Managing Director of Compass Consulting Group, an independent Internal Audit & IT Security Solutions provider. You can reach him at (210) 601-9710 or by email at [stonn@thecompassgrp.net](mailto:stonn@thecompassgrp.net).

