

## **Business Continuity Planning – Process and Framework**

Our last business continuity planning (BCP) article provided a discussion of recent FFIEC guidelines for BCP process-oriented planning and provided an overview of business impact analysis (BIA). This month we will focus on BIA concepts and activities in more detail.

### **Background**

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>

The guidelines encourage financial institutions to adopt a process-oriented approach for business continuity planning that involves:

1. Business impact analysis (BIA);
2. Risk assessment;
3. Risk management; and
4. Risk monitoring.

This framework is usable regardless of institution size and continuity planning should focus on all critical business functions that need to be recovered for operations resumption. Disaster recovery for technology alone should no longer be the primary focus of a BCP, but rather should be viewed as one critical aspect of the enterprise-wide process. The review of each critical business function should include the technology that supports it.

### **Action Summary for Management**

A business impact analysis is the first step in developing an effective BCP. Comprehensive BIA initiatives should include:

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers;
- Consideration of all departments and business functions, not just data processing; and,
- Estimation of maximum allowable downtime and acceptable levels of data, operations and financial losses.

The impact analysis phase of the continuity planning process identifies the potential impact of unanticipated disruption of the institution's business processes. The BIA phase also should determine what and how much is at risk by identifying critical business functions and prioritizing them. It should estimate the maximum allowable downtime for critical business processes, recovery point objectives and backlogged transactions, and the costs associated with downtime.

Management should establish recovery priorities for business processes that identify essential personnel, technologies, facilities, communications systems, vital records, and data. The BIA also considers the impact of legal and regulatory requirements such as the privacy and availability of customer data and required notifications to the institution's primary federal regulator and customers when facilities are relocated.

## **BIA Development**

Personnel responsible for this phase should consider developing uniform interview and inventory questions that can be used on an enterprise-wide basis. Uniformity can improve the consistency of responses and help personnel involved in the BIA phase compare and evaluate business process requirements.

This phase may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and maintenance of safe and sound practices. However, this prioritization should be revisited once the business processes are modeled against various threat scenarios so that the full BCP can be developed.

When determining a financial institution's critical needs, reviews should be conducted for all mission-critical functions, processes, and personnel within each department, and each department should document the mission-critical functions performed. Following is a list of questions suggested in the guidelines to be considered at the departmental level during the BIA phase of business continuity planning:

- What specialized equipment is required and how it is used?
- How would the department function if mainframe, network and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What is the minimum number of staff and space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What communication devices would be needed at a recovery site?
- What critical operational or security controls require implementation prior to recovery?
- Is there any potential impact from common recovery sites serving multiple lines of business or departments?
- Have employees received cross training and has the department defined back-up functions/roles employees should perform if key personnel are not available?
- Are emotional support and family care needs adequately considered?

## **Next Month – Risk assessment as part of BCP**

Stephen Tonn is the Managing Partner 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).

