

Risk Monitoring Needed for BCP

Our topic last month addressed implementation of risk monitoring through effective BCP testing. This month's article will provide an overview of specific guidance for a comprehensive test of your Business Continuity Plan.

Background

In May of last year 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. 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

Risk monitoring is the final step in business continuity planning. It should ensure that the institution's BCP is viable through:

- Testing the BCP at least annually;
- Subjecting the BCP to independent audit and review; and
- Updating the BCP based upon changes to personnel and the internal and external environments.

Risk monitoring ensures a BCP is viable through testing, independent review, and periodic plan updates.

Testing Scope and Objectives

Management should clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test. The objective of a testing program is to ensure that the BCP remains accurate, relevant, and operable under adverse conditions. Testing should include applications and business functions that were identified during the impact analysis. The business impact analysis determines the recovery point objectives and recovery time objectives, which then help determine the appropriate recovery strategy.

Testing objectives should start small, and gradually increase in complexity and scope. The scope of individual tests can be continually expanded to eventually encompass enterprise-wide testing, including vendors and key market participants. Achieving the following objectives provides progressive levels of assurance and confidence in the plan.

At a minimum, a clearly stated testing plan should:

- Not jeopardize normal business operations
- Gradually increase the complexity, level of participation, functions, and physical locations involved
- Demonstrate a variety of management and response proficiencies, under simulated crisis conditions, progressively involving more resources and participants
- Uncover inadequacies, so that configurations and procedures can be corrected
- Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services

Management should develop a test plan for each BCP testing method used. The test plan should identify quantifiable measurements of each test objective. The test plan should be reviewed prior to the test to ensure it can be implemented as designed without endangering the production environment. In addition the following areas should be appropriately considered:

Validation of Assumptions - The testing plan's assumptions should be validated to ensure they are appropriate for business continuity requirements. This validation requires the participation of appropriate business, operations, and technology staff.

Accuracy of Information - All documented data and lists in the BCP should be checked periodically for accuracy, including furniture, equipment, telecommunications connections, applications, and operating systems at both the primary and alternate sites. Version numbers of applications and operating systems should be specified on this list.

Completeness of Procedures - The test procedures should be checked periodically to make sure they include:

- Emergency response procedures, including escalation and notification processes
- Alternate processing procedures, including security procedures at an alternate site
- Full recovery procedures, including returning to normal processing

Testing Methods

Testing methods vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives, and benefits. The type of testing employed by a financial institution should be determined by, among other things, its age and experience with business continuity planning, size, complexity, and nature of its business. Examples of testing methods in order of increasing complexity include:

Orientation/Walk-through - An orientation/walk-through is the most basic type of test. Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP.

Tabletop/Mini-drill - A tabletop/mini-drill is somewhat more involved than an orientation/walk-through because the participants choose a specific event scenario and apply the BCP to it.

Functional Testing - Functional testing is the first type that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP.

Full-scale Testing - Full-scale testing is the most comprehensive type of test. In a full-scale test, the institution implements all or portions of its BCP by processing data and transactions using back-up media at the recovery site.

Conducting a BCP Test

Testing requires some centralized coordination, usually by the BCP coordinator or team. The team or coordinator is responsible for overseeing the accomplishment of targeted objectives and following up with the appropriate areas on the results of the test. Generally, it is advisable to

have the maximum number of personnel that will be involved in implementing the BCP also participate in the test. This participation increases awareness, buy-in, and ownership in achieving successful BCP implementation. It is also advisable to rotate personnel involved in testing in order to prepare for the loss of key individuals, both during a disaster and as a result of retirements, promotions, terminations, resignations, or re-assignment of responsibilities. The involvement and oversight of independent staff such as auditors will help to ensure the validity of the testing process and the accuracy of the reporting.

Remember, a useful test can only be achieved if the test results are analyzed and compared against stated objectives, and acted upon. Management should report the test results and the resolution of any problems to the board.

Updating Your BCP

A BCP is a “living” document; changing in concert with changes in the business activities it supports. The plan should be reviewed by senior management, the planning team or coordinator, team members, internal audit, and the board of directors at least annually. As part of that review process, the team, or coordinator should contact business unit managers throughout the financial institution at regular intervals to assess the nature and scope of any changes to the institution’s business, structure, systems, software, hardware, personnel, or facilities. It is to be expected that some changes will have occurred since the last plan update. Software applications are commercially available to assist the BCP coordinator in identifying and tracking these organizational changes so that the BCP can be updated. All such organizational changes should be analyzed to determine how they may affect the existing continuity plan, and what revisions to the plan may be necessary to accommodate these changes. The agencies expect that BCP updates will be documented to show that the plan reflects the institution, as it currently exists. Lastly, the financial institution should ensure the revised BCP is distributed throughout the organization.

Audit and Independent Reviews

The audit department or other qualified, independent party should review the adequacy of the business continuity process to ensure the board's expectations are met. This review should include assessing the adequacy of business process identification, threat scenario development, business impact analysis and risk assessments, the written plan, testing scenarios and schedules, and communication of test results and recommendations to the board. In order to discharge these responsibilities, the audit department or other independent party should directly observe tests of the BCP. The board should receive and carefully review audit reports on the effectiveness of the institution’s process that identify any areas of weakness.

Next Month – We will start our next series of articles summarizing recent FFIEC guidance – the April 2004 System Development and Acquisition booklet

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.

