

Risk Monitoring Needed for BCP

Our topic last month was use of risk assessment processes for development of the business continuity plan. This month we will provide an overview of regulatory guidance for risk monitoring as it relates to your business continuity plan. The primary risk monitoring process discussed in the regulations is BCP testing.

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. 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/ffiecinbase/html_pages/it_01.html

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,

Overall Testing Strategy

The development of testing strategies requires that you make a business decision regarding the level and frequency of testing needed to ensure recovery objectives can be achieved during a business interruption or disaster. The frequency and complexity of testing is based on the risks to the institution. Even small, serviced institutions should participate in tests with their core service providers and test other critical components of the BCP.

As we have stated earlier, comprehensive BCP entails more than simply recovering your information technology platform and resources. Planning for continuity of all critical processes must be considered. Therefore, only performing unmanned recovery testing, where back-up tapes are sent to the recovery site to be run by service provider employees, is not a sufficient BCP test in and of itself. Although this type of testing is clearly a very important part of BCP testing, it should be supplemented with testing of other critical aspects of the BCP. Testing strategies should detail the conditions and frequency for testing applications and business functions, including the supporting information processing.

The strategy should include test objectives, scripts, and schedules, as well as provide for review and reporting of test results. Management should ensure recovery testing is conducted at least annually, or more frequently, depending on the operating environment and criticality of the applications and business functions.

Types of BCP Testing

Management should evaluate the risks and merits of various types of testing and develop strategies based on identified resumption and recovery needs. The business continuity planning process should evaluate whether the institution is anticipating operating at full or reduced capacity. Financial institutions should not assume a reduced demand for services during a disruption. In fact, demand for some services (e.g., ATMs) may actually increase during disasters. If management plans to operate at a reduced capacity at an alternate site, risks should be evaluated for exceeding that capacity and priorities established as to what will or will not be processed.

Scope of BCP Testing

The process should also evaluate the necessity for enterprise-wide, service provider, and key market participants testing, rather than relying solely on isolated business unit testing. Comprehensive testing requires evaluating interdependencies between critical business functions and systems, and evaluating the criticality of testing those systems in tandem. Management should test its ability to recover current data from back-up media, and institutions should include security measures and procedures within the scope of the test, including ensuring secure copies of the back-up media remain available in the event of an actual problem during testing.

Next Month – We will wrap up the BCP series with specific guidance for BCP testing.

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.

