

Risk Assessment as Part of BCP

Our last business continuity planning (BCP) article provided an overview of recent FFIEC guidelines for BCP process-oriented planning and discussed issues related to Business Impact Analysis development. This month our topic is use of risk assessment processes in the business continuity plan.

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/ffiecinfobase/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

The risk assessment is the second step in developing a BCP. A comprehensive risk assessment should include:

- A prioritizing of potential business disruptions based upon severity
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives;
- An analysis of threats based upon the impact on the institution, its customers, and the financial markets, not just the nature of the

The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. If the threat scenarios developed are unreasonably limited, the resulting BCP may be inadequate. During the risk assessment step, business processes and

the business impact analysis assumptions are stress tested with various threat scenarios. This will result in a range of outcomes, some that require no action for business processes to be successful and others that will require significant BCPs to be developed and supported with resources (financial and personnel).

Threat Scenarios

Financial institutions should develop realistic threat scenarios that may potentially disrupt their business processes and ability to meet their client's expectations (internal, business partners, or customers). Threats can take many forms, including malicious activity as well as natural and technical disasters. Where possible, institutions should analyze a threat by focusing on its impact on the institution, not the nature of the threat. For example, the effects of certain threat scenarios can be reduced to business disruptions that affect only specific work areas, systems, facilities (i.e., buildings), or geographic areas.

Additionally, the magnitude of the business disruption should consider a wide variety of threat scenarios based upon practical experiences and potential circumstances and events. If the threat scenarios are not comprehensive, BCPs may be too basic and omit reasonable steps that could improve business processes' resiliency to disruptions. Threat scenarios need to consider the impact of a disruption and probability of the threat occurring. Threats range from those with a high probability of occurrence and low impact to the institution (e.g., brief power interruptions) to those with a low probability of occurrence and high impact on the institution (e.g., hurricane, terrorism). High probability threats are often supported by very specific BCPs. However, the most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence.

Gap Analysis

Using a risk assessment, BCPs may be more flexible and adaptable to specific types of disruptions that may not be initially considered. It is at this point in the business continuity planning process that financial institutions should perform a "gap analysis." In this context, a gap analysis is a methodical comparison of what types of plans the institution (or business line) needs to maintain, resume, or recover normal business operations in the event of a disruption, versus what the existing BCP provides. The difference between the two highlights additional risk exposure that management and the board need to address in BCP development.

Risk Assessment Components

The risk assessment considers:

- The impact of various business disruption scenarios on both the institution and its customers;
- The probability of occurrence based, for example, on a rating system of high, medium, and low;
- The loss impact on information services, technology, personnel, facilities, and service providers from both internal and external sources;
- The safety of critical processing documents and vital records; and
- A broad range of possible business disruptions, including natural, technical, and human threats.

When assessing the probability of a specific event occurring, financial institutions and technology service providers should consider the geographic location of facilities and their susceptibility to natural threats (e.g., location in a flood plain), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, points of interest, major highways, railroads).

The risk assessment should include all the financial institution or service provider's locations and facilities. Worst-case scenarios, such as destruction of the facilities and loss of life, should be

considered. At the conclusion of this phase, the institution will have prioritized business processes and estimated how they may be disrupted under various threat scenarios.

Next Month – We will wrap up the BCP series with an overview of risk monitoring needed for 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.

