INTERNAL AUDITOR

January 2008

The IT Auditor's Role in Business Continuity Management

Learning about their role in the business continuity management process can help auditors provide recommendations that will enable organizations to be one step ahead of the curve when disaster strikes.

Mark T. Edmead, CISSP, CISA
IT Director
Control Solutions International

During their planning cycles, many companies around the world evaluate how prepared they are to handle disasters as well as the effectiveness of their business continuity and disaster recovery plans. As part of this process, internal auditors can help organizations establish effective business continuity management (BCM) programs. To do this, auditors need to understand what is involved in developing a BCM program and the steps they should take to evaluate the effectiveness of existing programs that incorporate necessary business continuity, disaster recovery, and crisis management efforts.

DEFINITION OF KEY TERMS

Before auditing the organization's business continuity plan or providing recommendations that can enhance current and future business continuity efforts, it's important for internal auditors to understand the different components of the BCM process.

Overall, BCM is defined as the development of strategies, plans, and actions to protect or provide an alternative mode of operation for business processes that, if interrupted, could seriously damage or cause fatal losses to an organization. Hence, BCM processes provide a framework to ensure an organization's resilience to any event and to help ensure the continuity of services to its customers. In addition, BCM activities serve as the basis for plans that can help organizations ensure their long-term survival following a disruptive event.

Beside business continuity planning, BCM includes disaster recovery and crisis management. Following is a brief description of each.

Three Basic Elements of Effective BCM

In essence, a **business continuity plan** (BCP) addresses an organization's ability to continue functioning when normal operations are disrupted. This plan incorporates the policies, procedures, and practices that allow an organization to recover and resume manual and automated mission-critical processes after a disaster or crisis. Besides stating the practices that must be followed in the event of an interruption, some BCPs include other components such as disaster recovery, emergency response, user recovery, and contingency and crisis management activities. Therefore, in these organizations, business continuity is seen as an all-encompassing term that covers both disaster recovery and the resumption of business activities.

However, whether a part of the BCP or a separate document, **disaster recovery plans** (DRPs) should define the resources, actions, tasks, and data required to manage an organization's recovery process in the event of a business interruption. This plan also should assist a company when restoring affected business processes by outlining the specific steps the company must take in its path toward recovery. Specifically, the DRP is used for the advanced preparation and planning needed to minimize disaster damages and for ensuring the availability of the organization's critical information systems. In terms of IT, DRPs address the recovery of critical technology assets, including systems, applications, databases, storage devices, and other network resources.

Finally, **crisis management plans** (CMPs) enable organizations to effectively respond to an event. These plans are usually created as separate documents that can help organizations to stabilize a situation before recovery operations take place, as outlined in the DRP or BCP. In addition, CMPs discuss what systems are in place to quickly gather information about a disaster and how to interpret the information needed to prevent further confusion and chaos. Although not all disasters require the use of crisis management tactics, creating and implementing an effective CMP can help companies provide the necessary support that staff members need to cope with any stressful situations stemming from a disaster.

AUDITING THE BCM PROCESS

Given the wide reach of BCM activities, what is the IT auditor's role in the BCM process? First, the auditor needs to evaluate the organization's business continuity readiness on a regular basis and inform management of the evaluation's results. Therefore, the auditor needs to determine whether the BCM process enables the organization to maintain business operations in the event of a disaster. To this end, the auditor can perform a risk assessment to determine whether the BCM is addressing the company's most critical business processes.

In addition, the auditor needs to review the adequacy of the BCP, and DRP if separate, in ensuring the timely resumption of operations and determine whether these plans reflect the current operating system environment. In many organizations, the IT auditor also acts as a consultant during the development of the BCP and DRP documents and reviews the proposed plans in terms of their design, completeness, and adequacy.

During the scoping phase of the BCM process, the auditor also should perform a risk assessment to evaluate the established BCM framework, including the organization's due diligence in implementing the plan and whether all employees are being held accountable for the program's success. Furthermore, the auditor should evaluate whether the BCP and DRP plans meet recovery objectives (i.e., the compromised operation needs to be operational within the time frames set by senior management). An important consideration to keep in mind is whether the organization has identified all of its critical business operations. For instance, some companies have a BCP in place, but the plan does not focus on critical business processes. The auditor, therefore, must determine if all business continuity objectives are aligned with companywide operations.

BCM AUDIT COMPONENTS

After the organization has an established BCM process, the IT auditor can review the plans, controls, and processes that are in place to support it. The audit fieldwork phase looks similar to any audit project. Key actions that need to be performed during the audit include:

- Conducting interviews with management and other company stakeholders to determine their involvement in business continuity planning efforts.
- Reviewing the BCM document to determine its completeness, accuracy, and timeliness.
- Reviewing supporting BCM documents, such as procedural manuals, guidelines, and training materials.
- Evaluating the effectiveness of BCP and DRC plans by reviewing plan testing results or the results of actual disasters where the BCP or DRP was used. This can be accomplished by asking questions such as: Did it work? What worked and why? What did not work and why? Was the process improved?
- Analyzing the audit report's conclusion and recommendations.

The IT auditor also should be involved in the recovery period. This is an ideal time to evaluate the entire BCM process. During the recovery period, the auditor can monitor the effectiveness of companywide recovery and control operations, recommend improvements, provide support during recovery activities, and assist in identifying lessons learned. Here are some questions the IT auditor can ask during the audit of the BCM process:

- Are the plans up-to-date?
- Are all critical systems and business functions included in the plan?
- Are the plans documented?
- Have responsibilities been assigned?
- Are the plans based on a risk assessment?
- Are the plans tested and revised based on plan test results?
- Where are the plans stored, and are they stored safely?
- Do plan action steps coordinate with local emergency services?
- Are alternate data center locations known to everyone?
- Do you know where data backups are located?

- Does the organization have adequate staff to implement the plans?

Answering these questions can help auditors evaluate the effectiveness of companywide BCM processes and provide recommendations that can help organizations to better address their business continuity needs.

MORE THAN JUST AUDITING

As organizations continue to change, so do the roles of IT auditors. In many companies, audit roles and responsibilities are already expanding to include more proactive reviews and audit involvement in the BCM process. To effectively audit BCM activities, auditors must understand the objectives and scope of companywide business continuity activities. Additionally, auditors need to look at existing business continuity and disaster recovery plans from a process perspective and not treat the audit as a documentation review. Consequently, business continuity should be treated as a management process that incorporates feedback from various departments and functions (e.g., senior management, human resources, and operations), as well as business activities such as risk assessments. Ultimately, the goal of any BCM process is to ensure the consistency and awareness of companywide business continuity, disaster recovery, and crisis management activities.

For additional information on the BCM process, auditors can visit:

- The ChicagoFIRST Initiative.
- The *IT Continuity and Disaster Recovery newsletter*.
- The Directors and Boards Web site and read *Boardroom Briefing's* Business Continuity and Disaster Recovery issue (PDF).
- The SANS Web Site and read "Preparing for A Disaster: Determining the Essential Functions That Should Be Up First" (PDF)

Mark Edmead is the IT director of Control Solutions International and has more than 25 years' experience in the areas of computer systems architecture, information security, project management, and IT and application audits. In the past, Edmead worked as a consultant for Fortune 500 and 1000 companies in the areas of information technology, systems, and Internet security, as well as regulatory compliance.