Internal Audit's Role in Business Continuity

By Jack Bess, KnowledgeLeader contributing writer

On a March 6, 2007 Institute of Internal Auditors (IIA) web cast, four panelists spoke about the important role internal audit plays in an organization's business continuity efforts.

Without well-thought-out plans for recovering from a disaster and restoring vital business functions, an organization exposes itself to the risk that it may not be able to survive a major disaster. Aftershocks of the September 11, 2001 terrorist attacks (9/11) on the World Trade Center and Hurricane Katrina, for example, have led to heightened awareness of the vulnerability of business operations.

As part of the rising tide of awareness, internal auditors are starting to understand that they have an important role to play in ensuring that their organization has an effective and well-tested business continuity plan. With their broad knowledge of how an organization works, their intellectual curiosity and independence, internal auditors bring a unique and valuable perspective to the process of planning for the impact of a business interruption.

Developing a business continuity plan can seem like daunting work, but it is a task that is a natural extension of internal audit's mission, says Molly Latham, business continuity planning manager at Southern California Edison. "Internal audit has always had a role to play because at its heart, business continuity is an internal control, and that is what auditors are concerned with," Latham said.

Business continuity basics

The growing awareness of how important it is to plan for business continuity mirrors the evolution of disaster recovery as a discipline. Historically, "disaster recovery" was considered the province of Information Technology (IT) departments grappling with the issue of how to recover critical systems.

However, as companies grew mature about recovering technology, "technical people started realizing that just because we can bring the computers back does not mean we can bring the business back," Latham says. Recognizing that technology was just one piece in a larger process of recovering business functions after a disaster, disaster recovery morphed into the larger discipline of business continuity, and business continuity ownership has tended to shift from IT to the corporate level, she says.

In addition, the trend toward globalized operations has underscored the importance of continuity risks, which now appear more frequently in enterprise risk assessments, says Michael Keating, associate director of technology risk at Protiviti.

"Increased consolidation, outsourcing and offshoring create risk concentrations that have to be monitored and mitigated frequently," Keating continues. "I have met people who believe that because they have outsourced some operation that somehow the continuity exposures are not there anymore. In reality, the exposure is still there, but they have less direct control over it."

Increasingly conscious of business continuity, major companies such as Starbucks and manufacturer Callaway Golf have listed pandemic influenza as a continuity risk in their 10-K filings with the U.S. Securities and Exchange Commission, Keating says.

Raising the stakes still higher for companies are heightened expectations that businesses are taking appropriate steps to address disaster-related risks, Keating says. External auditors now ask about business continuity risks in areas beyond financial reporting, he notes.

Customer mandates are also raising the bar for business expectations, says Edison's Latham. "Customers are asking businesses about their pandemic plans," she says. "They are requiring companies to do these things as a condition of doing business with you."

Then there is the emergence of new disaster-recovery standards, in particular, the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs. Complying with Standard 1600 is not a requirement, but the 9/11 Commission has recommended that 1600 be the benchmark for a company's performance, Keating says.

"There is now greater director and officer exposure to failed continuity," Keating says. "This is not a standard that is required to be complied with right now; but if there is a failure of continuity of business and if there were a shareholder suit or some other activity, this would be the benchmark by which your organization will be measured."

This is the backdrop against which internal auditors are performing. While this opens the door to new challenges and new depth of activity, the emerging standards represent good news for auditors in that "we know now what it is we should be auditing against, as opposed to just making judgment calls in areas where we might not necessarily have any experience in business continuity," Keating says.

Methodologies and tools

According to some experts, the National Preparedness Standard is an excellent place for internal auditors to begin its exploration of business continuity management tools, serving as an outline upon which further refinements can be added.

Another helpful tool – the "gold standard," according to Keating – are the Federal Financial Institution Examination Council's business continuity guidelines, which include clearly laid-out descriptions of the roles senior management and the board can take.

"The 'gold standard' requires that reasonable efforts be made on a whole host of fronts," Keating says. "But in order to say you have made a reasonable effort, you need to have a basis to say something is reasonable or is not reasonable."

While it is not strictly necessary to consult multiple methodologies, keeping informed about other standards is a good professional practice, says Edison's Latham, a former auditor. While there might be some duplication of ideas, one plan might place heavier emphasis on technology, and another on emergency management, both of which help illuminate various aspects of continuity planning, she says.

Latham says she has found value in guidelines from the Virtual Corp., DRI International (which certifies business continuity professionals) and, especially, the heavily detailed British Standard BS 2599, which has helped her scrutinize Edison's business continuity plan with greater granularity. Using the British Standard may reveal a number of weaknesses, for example whether or not an audit has been performed recently, she says.

Keating also recommends becoming familiar with The IIA's Practice Advisory 2110-2, which supports internal audit's role in the business continuity process.

In addition, Keating describes how the essential elements of a business continuity plan should include governance (Who are the owners and how are they held accountable?); an analysis of the impact of a business interruption (How bad does the pain get and how quickly?); identification of resources necessary for a business recovery; an actual strategy that can be deployed in the recovery; tests to ensure that the plan is adequate for the task; ongoing maintenance; and a process of independent review or auditing of the plan.

Keating stresses the need for formally documenting the plan, saying that some clients insist that the continuity plan is "up here, while pointing to their head." In that regard, an effective continuity plan should be as clear and practical as a cookbook, Latham says. "You want people to be able to pick up that document and go through the steps," she said. "It needs to be targeted to what people need to do; who would need to do them; and what order they need to be performed to recover from the disaster."

Putting it down on paper gives auditors a chance to study the plan at length and determine whether the unstated assumptions are valid, Latham and Keating observe. For instance, a plan might assume that the most knowledgeable people in the company will be available in a disaster to lend their expertise.

"The experts may be on the other side of that bridge that collapsed and they cannot be on the scene," Latham says.

It is not necessary that continuity plans be developed for every scenario, whether terrorist attack, earthquake or flood. The point is to address the conditions that will prevail in a disaster.

"Normally, business continuity is hazard-neutral, so it does not matter why the business is interrupted," Keating says. "You want to have plans in place to address the interruption so you know the tolerance for impact. Some people can do nothing for weeks and there is no material impact, but if you are an auto manufacturer, you start to feel the pinch in a few hours."

Any continuity plan should be measured so a company knows whether or not it is as thorough as it should be, Latham said. Metrics include the plan's testing, the frequency of testing, the meeting of test objectives, recovery time objectives, and levels of employee training in disaster response, she says.

Ultimately, Keating says, "It is not the job of a business continuity program to insulate the company from every possible risk since companies decide to assume risk all the time. It is the job of the business continuity plan to insulate the company from those risks that have a material impact on the financial statements."

Testing makes the difference

Acknowledging that "we are not always experts at every process we audit the first time we audit it," there is "quite a bit of homework" auditors need to do to prepare for auditing a business continuity plan, says Matthew Gagnon, former vice president and director of internal audit at Fieldstone Investment Corp.

This homework can be divided into three main areas of focus: preparation of a high-level estimate of the scope of the business continuity plan (BCP) audit; obtaining approval for including the BC audit in the existing audit plan; and planning and executing the audit engagement.

Preparing a high-level estimate of the scope

This will help determine the level of resources needed for a BCP audit. In preparing the estimate, Gagnon said, you need to consider the BCP's maturity. Does a formal BCP even exist? Has an up-to-date Business Impact Assessment been performed? Getting into the depth of detail will depend on your ability to document and prioritize specific risks relevant to the audit and the organization itself. With this estimate in hand, auditors should develop an actual audit program that can be scoped and inserted into the audit plan, he said.

Take note of The IIA's Standard 1220 on Due Professional Care, Gagnon says. "It is very important for you to understand that – not in this or any other audit – do you need to test every risk and control," he says. "You are encouraged to consider, among other things, the cost of assurance relative to the potential benefits."

Obtaining approval for the BCP

When auditors present their BCP to management and to the Audit Committee for approval, it is possible that approval will not be given. If you conclude that not assessing BC risks presents an unacceptable risk to the organization, "according to the standards, you are to report this to management, and if they do not resolve the situation, you are to report it with management to the Audit Committee or to the board for resolution," Gagnon says.

Planning and executing the audit engagement

Once the BCP is incorporated in the audit plan, auditors need to document their understanding of the BCP's objectives, the owners and participants in the process, and the current state of the disaster plan (Has the Business Impact Assessment been performed, and so on.)

"Because of the sheer breadth of the BCP, auditors may want to take this opportunity to discuss the value of Enterprise Risk Management (ERM) with management," Gagnon says. "An effective BCP involves at least three of the ERM framework's eight elements: event identification, risk assessment and risk response. If these elements are not in the BCP, auditors may help 'coach' management in their identification of the three factors."

"The IIA considers it appropriate for internal auditors to take on the roles of coaching and coordinating the ERM process, as long as you have a process in place to transfer ownership back to members of management, with a clear timeline for that transition," Gagnon continues.

In defining the business objectives and scope of the BCP, it is very critical to have management's perspective on the process dependencies, which is essential to understanding the proper recovery sequences, Gagnon says. "For example, your recovery time objectives should not be established without considering the upstream and downstream impact of business disruptions on the business process, the systems and on the third-party service providers," he adds.

The extent of testing will be determined by the complexity and structure of the BCP, which would include a Disaster Recovery Plan (concerning business applications, hardware, IT infrastructure and connectivity); a Business Resumption Plan (recovery of business operations and corporate functions); and Crisis Management (the BCP oversight plan that includes the communications plan).

"Testing is where the proof of the effectiveness of the plan can be found," Gagnon emphasizes.

Takeaways from 9/11

"The disaster you plan for is not the one you get. So you have to make sure your plan is flexible, that people know it and that they communicate at all times."

Those are hard-earned words of advice from Kevin Piccoli, executive vice president of The Bank of New York Mellon Corporation, whose world headquarters, 8,300 employees and its data, operations and trading centers were impacted by the attacks on the World Trade Center.

While the bank had business continuity plans in place on 9/11, the magnitude of the disaster was something no one could have anticipated, Piccoli, who was the chief auditor at the time of the attacks, says. Still, the bank's internal auditors, with their unique holistic view of the organization and their detailed, thought-through understanding of business processes, brought a "huge added benefit" to the bank's recovery effort, he said.

"Auditors understand how things happen and why they happen the way they do, and they can use that knowledge to build workarounds or to fill the knowledge gaps if key people are not available," he says.

The auditor's depth of knowledge of all strata of the organization, from the clerical to the corporate levels, assists in the "fluid, constant redesign of the continuity plan" in the heat of a disaster response, he adds. Internal auditors act as the "eyes and ears" of management during the recovery effort. They can spot a troubling lack of resources in one area or raise concerns if someone is relaying to top management an unrealistically rosy picture of what is happening in the trenches, Piccoli says. Upon spotting problems, auditors can relay that critical information to make sure that the right decisions are being made at the top, he says.

Diversifying the bank's communication plan is probably the most significant change resulting from the 9/11 experience, Piccoli says. In the immediate aftermath, cell phones did not work, he says, which underscored the need to have pre-established 800-numbers to a land line. Furthermore, it was important to communicate with employees to reassure them that delivery of their paychecks and benefits was not impacted.

Clear, quick communication also plays a critical part in reassuring customers and Wall Street observers that the bank is on the track to recover, Piccoli says. One striking post-9/11 problem occurred when the media reported that Bank of New York's ATM machines were not operating. In its business continuity planning, the bank had determined that customers could access their accounts through other banks' ATMs, and Bank of New York would waive the service fees. That seemed like a reasonable solution until those press reports about bank machines, Piccoli said, which sent inaccurate impressions about the bank's recovery efforts to customers and to Wall Street, at a painfully sensitive time when rumors were flying.

"They were not reporting that we were successfully clearing $1 trillion a day in cash and securities movements but that the ATMs were not up and running," Piccoli says. "So we needed to modify our plan and just get our ATM network up. We had to make sure our plan was fluid enough for us to be able to react and re-prioritize."

Ultimately, the 9/11 experience has sparked a greater appreciation for greater depth of business continuity planning, Piccoli says.

"I think auditors are much more appreciative of the fact that if we do not really have this nailed down tight and we have a disaster, we are in trouble," he concludes.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.