

Taking the Risk out of IT

(May 1, 2008)
By Robert W. Scott

|

There is little better measure of how hot the demand for risk management services is than the experience of Brown Smith Wallace in the first quarter of this year.

"We have closed so much work in the first quarter that we have almost reached our quota for the year," says Tony Munns, one of the co-leaders for the risk management practice at the Saint Louis-based accounting firm.

Spurred by regulations, and by the increasing reliance on technology by virtually all businesses, the need for a wide array of services that help companies reduce risk has mushroomed over the last few years.

The firm's Web site lists the services as data analysis service, enterprise risk, Sarbanes-Oxley assistance, SAS 70 and third-party assurance and technology risk.

Risk assessment engagements "go in all directions. We have been asked to perform risk assessments because there was fraud or because someone lost a laptop with critical data," says David Smokler, director of technology for the governance practice at Roseland, N.J.-based J.H. Cohn.

"We have two IT risk methodologies," says Smokler. "One of them is primarily focused on internal auditing engagement." The other is the IT diagnostic risk assessment, which involves looking at an entire organization and all technologies.

Risk within a company's technology system can occur for reasons other than the normal threats posed by viruses, hackers and thieves. Problems can occur because as an organization's IT infrastructure expands, it can deviate from the original architecture. Acquisition of new companies can also introduce risk.

"When you acquire a new division and are in the progress of migrating data, there is inherent risk to the individual company," says Smokler. One of Cohn's tasks is to recommend standardization that will give the company more control over its processes.

The tools used by Cohn and other firms rest more on processes than on software, although many have developed their own tools and some commercial products such as ACL and CaseWare Idea are commonly used.

In Cohn's case, a three-phase process is used by the staff of more than 30 that studies "anything that plugs into the wall," in its definition of technology.

Risk and Rewards

The more business becomes automated, the more work there will be for the professionals who perform risk assessment.

"There is much more need to have more boxes [computers] do things," says Brown Smith's Tony Munns. He notes that even the doctor's office is increasingly automated with physicians walking around while holding computing devices, and with computers in use by police.

And with the drive to develop digital images of documents, enabled by low cost for storage, there is an increasing amount going onto the devices in

In Phase I, the firm builds an asset-based profile. It develops an understanding of senior management and a company's operational areas and the knowledge of the staff.

Infrastructure vulnerabilities are identified in Phase II and “we go through the process of evaluating various tools that are specific to the company's environment,” Smokler says.

In Phase III, the firm puts together the strategy and plan and conducts analyses.

“What makes Cohn different is that, not only do we have the capabilities of using testing tools,” says Smokler, “we have the capability of understanding how to analyze the output.”

Where Companies Fail

Despite the fact that Anchin, Block & Anchin performs a lot of risk assessment and IT audits for public companies that need to comply with Sarbanes-Oxley and private organizations that need SAS 70 audits, the IT problems found are often surprisingly basic.

“It's about password control and maintenance. It's change management. It's making sure you have the proper environmental controls with air conditioning and fire suppression, making sure the doors to the server room are locked,” says John Dodge, managing director of business risk services for the New York-based accounting firm.

In fact, most of the recommendations Anchin issues don't involve sophisticated technical issues—they are recommendations for taking care of basic issues that companies ignore or forget to deal with.

One precaution that can easily be overlooked is making sure servers are under warranty. Typically, a company might have servers that are six years old that have been out of warranty for three years.

“These are the kinds of things companies take for granted,” says Dodge. “Some of these organizations have been very fortunate that they have not experienced a server failure.”

And, of course, organizations that back up data frequently fail to test the backups to see if they will actually restore the information.

“This is exactly the kind of thing we run into frequently,” says Dodge. “The IT department has procedures, but there are breakdowns in their own processes that allow these mistakes to occur. If that occurs at the server level, you can imagine the risk.”

Tighter Ships

For the four-year-old risk management technology group at BKD, its banking and financial services clients generally have sophisticated controls on their technology systems.

businesses throughout the world.

Munns still sees the horror stories, such as a client who was found to have sent out blank backup tapes for a month because nobody looked at the log to see if the job was actually being performed. Then, there was the executive who was asked the last time he had backed up his laptop and couldn't remember.

“You have to save people from themselves, the system has to be automated,” he continues.

Ironically, Munns does not see the move to outsourcing computer functions as decreasing risk. Organizations must still see if contracts require the service provider to have a disaster recovery plan and to test it.

Executives often see outsourcing as a way to avoid costs. But since the providers are also “there to make money at the least possible cost, you have to have more sophisticated IT people, because you have to have people to manage the contract.”

The key to solving these technology problems is not just technology, Munns says. It's providing the people, such as the CISA and CISSPs who work in these practices, up to date.

“The need for a knowledge base and experience is huge,” says Munns. “You've got to be prepared to invest in your people. We have fought this battle too many times. Partners will consider CPE as an expense. They don't understand that it is an investment in the future.”

The other major issue is providing training to the next generation working its way through career paths at the firms so that there will be leaders ready to run these practices.

“A lot of midsize companies are facing the fact that most partners are now well into their 50s,” he notes.

"Typically, things are pretty tight," says managing consultant Ron Holshizer, who describes the group as a virtual practice that draws upon expertise from all of the firm's offices.

Prior to the formation of the unit, there were pockets of expertise spread around the firm. Since then, the practice has grown very rapidly. Holshizer attributes that to the fact that "the reliance on technology is so much greater than it was five years ago. If you lose your systems, things come to a screeching halt."

The most common engagement performed by BKD is a generalized IT controls review that encompasses a comprehensive study of technology controls, policies, processes, personnel control, software development life cycle controls and business continuation and disaster recovery.

When banks are clients, the controls involve a high degree of reliance on their vendors, who generally have a high degree of technical expertise.

"We don't run into too many problems," he says.

That's when it comes to networks and other systems under direct IT control. It's a different story when it comes to portable devices, including laptop computers and cell phones.

"These are the ones that concern us. You don't know if the loan officer has taken the laptop home at night," he says. However, most financial institutions have encrypted hard drives and communication between remote sites and offices are via virtual private networks. Most also have extensive policies and procedures.

IIA Issues Guide for IT Risk Assessment

The Institute of Internal Auditors has issued a Guide to the Assessment of IT Risk that is built upon a five-step program for identifying trouble spots within a company's IT system

These involve identifying critical IT functionality; the significant application where IT general controls need to be tested; IT general control process risk and related control objections; key IT general controls to test that meet the control objects; and performing a "reasonable person review."

The organization also issued an eight-step GAIT-R Methodology that starts with understanding the audit's review purpose or controls assessment and ending with a defined scope of work. The steps are the following:

1. Identify the business objectives for which the controls are to be assessed.
2. Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.
3. Identify the critical IT functionality relied upon, from among the key business controls.
4. Identify the significant applications where ITGCs need to be tested.
5. Identify ITGC process risks and related control

What concern about security has produced is “redundancies on top of redundancies,” to make sure data is safe. Clients will have mirrored systems on site, back up to tapes and take information off site.

The firm also deals with a people issue involving technology—phishing, the effort by outsiders to dupe computer users into revealing critical information such as bank account and bank routing numbers and Social Security numbers.

objectives.

6. Identify the ITGC to test that it meets the control objectives.

7. Perform a reasonable person holistic review of all key controls.

8. Determine the scope of the review and build an appropriate design and effectiveness testing program.

Simply having the accounting firm team come in and ask employees questions about their practices helps.

“They behave differently if they know somebody is looking over their shoulder,” says Holshizer.

More Help

One element that will help clients and auditors improve compliance is the move to build better tools into commonly used accounting packages.

Microsoft’s adoption of role-based computing can help because it enables companies to keep roles and responsibilities separate, according to Craig Dewar, director of community marketing for Microsoft Business Solutions.

Dynamics GP, AX and SL increasingly offer pre-defined roles. Roles will be available in the next version of Dynamics NAV.

Roles are defined so that users can see only the information necessary for them to perform their jobs. For example, someone in accounts receivable couldn’t see information in inventory.

In remarks made at Microsoft’s Convergence user conference in Orlando in March, Dewar discussed the introduction of the compliance center dashboard, which provides access to reports that are built via SQL Reporting Services.

“This gives me a very simple look at the effectiveness of my controls and the key performance indicators that I would like to track,” said Dewar.

Automating the process is also at the core of the work done by Thomson Tax & Accounting’s PPC organization in helping accountants comply with new risk standards, according to Cheryl Stydnicki, senior product manager for PPC audit and accounting.

The company first released its e-Practice aids in October 2006, which took the PPC audit approach with which many firms were familiar, by making an automated tool that walks the user through the audit process.

“We use risk assessment technology to generate customized audit programs based on risk assessment,” notes Scott Spradling, PPC’s senior director of product development.

Spradling says the e-Practice aids walk the user through the process, considering company structure and the role of each individual operating within the company. It also poses a series of planning consideration and questions.

“Different companies have different risk areas,” says Spradling. “It’s up to the user to identify the particular risks.”

Use of XML files also means that audit guidance from PPC can be fed into what the company calls a smart platform.

“We typically will update that information on an annual basis,” says Spradling. Updates include additions from PPC’s editorial staff working along with input from outside authors.

PPC is developing a series of modules to cover the entire audit, with Internal Controls the next module planned for release. Spradling says that is designed to “walk through a top-down assessment of the internal control system,” in line with standards from bodies such as the SEC and PCAOB.

Robert W. Scott is Editor of Accounting Technology and can be reached at Robert.scott@sourcemediacom.com.

THE LATEST ON WEBCPA

[Orrtax Changes Name to IntelliTax](#) - WebCPA (May 2, 2008)

[WebCPA Breaking News Roundup](#) - WebCPA (May 1, 2008)

[Conferences 2008: Fill 'er Up?](#) - WebCPA (May 1, 2008)

[Keenan Pitches Outsourcing to CPAs](#) - Accounting Technology (May 1, 2008)

[AccuFund Reaches Out to Neighbors](#) - Accounting Technology (May 1, 2008)

[More Related Articles](#)

Roaming Laptops: The Greatest IT Danger

With all the worry about hackers, phishers and thieves, the biggest problem in keeping data safe is still laptops left in cars or other locations by employees. At that's true of government agencies, private companies and accounting firms.

“That is our biggest issue, maintaining security of physical laptops. The issue of encrypting is also one part of the equation,” says Suzanne Holl, vice president of loss prevention for Camico. “Many times, people don’t remember what was on the laptop.”

Whatever happens, clients should be notified that there is a breach. Much of the worry about lost laptops can be assuaged if companies encrypt the data. And increasingly there is a big push for organizations to utilize technology that will let them remotely wipe the hard drive when a laptop is lost. Such technology is already utilized for disabling handheld devices.

However, despite the high-profile cases in which laptops containing information on hundreds of thousands of people have been stolen, Camico has not had a case related to someone who was damaged as the result of having such information contained on a stolen laptop.

“A lot of the theft involves people who are looking for the hardware—not for the information contained in it,” she continues.

For accounting firms that provide technology services to clients, many of the steps taken by organizations that perform risk assessment are good practices.

That includes documentation of systems installed and establishing scope and limits in engagement letters.