[Feature]

Do-It-Yourself Auditing

Although it might make sense to perform IT audits internally, tread carefully.

By Karen D. Schwartz


Embedded image: Dick Patrick / Jupiter Images

When information technology veteran Mark Friedman joined Virginia Commerce Bank three years ago, he inherited several systems, applications and controls that, although functioning well, were not monitored effectively. Friedman's predecessor had conducted a general yearly audit, but it was less than comprehensive and needed overhauling.

During his first year, Friedman, vice president of general audit at the 270-employee company, chose to outsource several portions of the IT audit because of time and staff limitations, as well as the lack of internal expertise. Three years later, he has made great progress in shoring up the Chantilly, Va., bank's auditing processes and procedures, using standard methodologies and technologies when possible. Today, much of the IT auditing is performed in-house.

For small businesses, such as Virginia Commerce Bank, with the right mix of executive commitment, IT personnel and auditing expertise, it is possible to perform system reviews in-house. All are key factors to a successful internal IT audit, experts say.

Small businesses that aren't subject to a host of government regulations also have an easier time of going it alone. On the flip side, businesses in highly regulated sectors, such as health care, which must comply with the Health Insurance Portability and Accountability Act, and financial institutions or companies with large finance departments, which must comply with the Sarbanes-Oxley Act, often need outside experts versed in those specific regulations to perform at least part of their IT audits.

First Things First

Once executives and the IT team determine that performing a systems audit internally is manageable, the next step is figuring out where to begin. To get a handle on what to audit, consider starting with a standard audit checklist provided by organizations such as AuditNet's Auditors Sharing Audits Programs (www.auditnet.org) or the Information Systems Audit and Control Association (www.isaca.org). Because information security is a consistent thread throughout all IT audits, many organizations use a framework specifically for the information security component of the review. Some examples are the Control Objectives for Information and related Technologies developed by ISACA and the IT Governance Institute (www.itgi.org) or ISO 17799, the International Standards Organization's set of controls comprising information security best practices (www.27000.mobi).

» comment
» print
» email
del.icio.us
digg this
rss feeds

RELATED | MOST POPULAR

Small but Strong
Wyse Technology's V10L thin client packs power in a small footprint.

The Right Switch for the Job
Considering what you get for the price, the D-Link DGS-2205 is a perfect switch for your small office/home office.

Windows Vista Comes of Age
Take a look at improvements to Windows Vista, available in the forthcoming Service Pack 2.

Helping the Help Desk
These days, computers are essential for day-to-day operations. Follow these tips keep your help desk moving in the right direction.

Reducing Costs With Microsoft Infrastructure Optimization
Microsoft IO provides a simple structure for evaluating the efficiency of core IT services, business productivity and application platforms.

Citrix NetScaler 9
NetScaler 9 includes integrated caching and compression to help network engineers get the most out of the bandwidth they have.

Be the Driver, Not the Driven
Don't let the inertia of day-to-day systems demands grind innovation by the IT team to a halt.

Mix It Up
Adhere to the four commandments of security — deter, detect, delay and respond — with blended physical and technology security teams.

Uncommonly Parallel
Five IT chiefs offer smart tips for keeping technology costs down and alignment with business goals up in a tight economy.

Practice What You Preach
Techies from green technology startups reveal the consumption-minded measures the companies take internally.

Other sources of security help include the Institute of Internal Auditors (www.theiia.org), the National Institute of Standards and Technology (csrc.nist.gov) and the Carnegie Mellon Computer Emergency Response Team (www.cert.org).

Choosing the right person to lead the IT audit is crucial, too. Large companies often have chief audit officers, but small companies often leave internal IT auditing to the CIO, an IT director or even the CFO. This isn't necessarily a bad idea, but it's important to prevent conflicts of interest that can compromise the audit and the business, says Herriot Prentice, director of technology practices at IIA in Altamonte Springs, Fla.

Photo: Steven Widoff

Make sure to choose the audit team wisely, says the Institute of Internal Auditors' Herriot Prentice, because "you want to ensure that it's as impartial as possible."

"If you're going to do [an audit] in-house, be careful who is in charge because you don't want to cross any lines, and you want to ensure that it's as impartial as possible," says Prentice. He cautions against having internal auditors overseeing reviews of their own departments. "If someone is responsible for technology, for example, and there is a technology audit going on, how independent are they going to be? Reporting lines can be strained."

Step Up to Success

Although it seems obvious, the best way to succeed on an internal IT audit is to understand what you are auditing.

"What does the organization wish to accomplish with the audit? Is it to assess the current risk levels against a target goal, or to confirm compliance to a specific regulatory mandate or other compliance initiative? The important thing is to be clear about what the organization wants to achieve during the audit process," says Diana Kelley, vice president and service director for security and risk management strategies at Burton Group, an IT infrastructure consultancy in Midvale, Utah.

The first step in engineering an effective audit is to separate the layers of IT and make sure the audit addresses each: IT management, technical infrastructure and applications.

IT management typically includes systems monitoring (identifying corrupt data-bases or transactions that failed to post because of errors), pinpointing programming errors, strategic planning and governance. The technical infrastructure covers general computer controls, such as operating systems, databases and networks. The final layer consists of transactional and support applications, while the final layer consists of external connections, including the Internet and connection to provider networks via other means, such as electronic data transfer.

For each layer, identify the associated risks for availability, security, integrity, confidentiality, effectiveness and efficiency. After identifying the risks, it's time to decide which type of IT audit should be performed. If, for example, a company relies heavily on wireless networks, it makes sense to include an audit of those networks.

Security is particularly important, notes Jeff Rudolph, partner in charge at Sikich Technology, an Aurora, Ill., firm that performs IT audits for companies of all sizes. "Small businesses think that because they are small, they aren't targets, but that's just not true. Any vulnerable network is a target," he says.

In deciding the types of IT audits to conduct, Virginia Commerce Bank made its decisions based on the business units affected by them. To determine which systems controls should be part of the audit, Friedman started culling the controls from the information service group's policies and procedures manual. Once he had compiled a list, Friedman and his team met with department managers, who explained their control points and how things work. "From there, we knew what the controls for the audit should be," he says.

Red Flags

As an audit progresses, IT auditors are looking for anything that raises a red flag, such as outdated patch levels, service patches or unauthorized access to sensitive systems. Just recently, for example, Friedman found during a routine audit of the general ledger system that the CFO had the ability to make specific changes that were supposed to be limited to just a few senior people. Although temporary access might have been granted for a specific reason, it was Friedman's responsibility to reinstate rights privileges — in this case, preventing the CFO from gaining access to the system.

At Nace International, a Houston corrosion engineering association, the systems team conducts one annual audit and an interim checkup, systems administrator Pam Nicoletti says.

"We do a software and hardware audit, so that we know what is installed," she says. "We lock down our systems, but some end users still install unauthorized software."

Photo: Rocky Kneten

Auditing lets Nace International make sure that no unauthorized software makes its

At midyear, Nace does an electronic audit of its computers, but for the annual audit, IT personnel run an inventory on each machine to make sure that nothing is missed. "We're very serious and proactive about ensuring that we only run licensed software," Nicoletti says.

So, what criteria make a small business likely to perform successful IT audits?

Educate yourself and your audit staff, IIA's Prentice urges. "Any competent auditor should possess a certain skill set and have certain designations. Take classes and get certified."

Prentice also stresses the need for commitment from top brass. "Within any organization, the appetite for an

audit has to come from senior management. If they take it seriously, it will succeed, but if they don't believe in the benefit of internal audits, it won't.

way onto systems, systems administrator Pam Nicoletti says.

"Expectations are a two-way street, and management should work with the auditors to ensure that both sides are working together and understand each other," he says. "Business managers should be prepared to provide auditors with a well-documented description of the business unit or program, including its key policies, procedures and ongoing efforts to succeed."

Communication is key, agrees Gabriel Fuchs, an IBM consultant who performs audits for companies of all sizes and previously conducted internal IT audits while on the staff of a Swiss insurance company. "Any organization with a culture of open communication and a true spirit of working toward the same goals will have a better chance of success," he says. "Culture is a soft factor that isn't easy to measure but nonetheless is a key to success."

In some ways, in fact, small businesses may have the edge over their larger counterparts when it comes to effective IT auditing, Fuchs says.

"Small businesses have the advantage of being much more responsive to business needs, as the key people in both business and IT tend to work more closely together than at larger organizations," he says.

Annual Checkup, Interim Tune-ups

Small businesses that aren't subject to specific regulations usually perform general IT audits once a year.

The Burton Group recommends that internal audit teams ideally should review high-consequence systems **quarterly**, medium-consequence systems **twice yearly** and low-consequence systems **yearly**. The report notes that any significant changes to high- or medium-risk systems also demand an **immediate review**.

When deciding **what to audit**, here are a few systems and processes that are ripe:

1 Systems and device inventory (type and number), including software, hardware and patches

2 Return on investment on projects run by IT

3 Help-desk calls, duration and case closure rates

4 Automation levels for system maintenance — i.e., the operations that run the IT applications

5 In-house development and its total cost of ownership compared to projects of existing off-the-shelf prepackaged solutions

6 Productivity levels of consultants versus employees in the IT department

7 Budget of IT costs versus actual expenditures

8 Number of different platforms and databases, and if and how they are able to communicate with each other

9 Networked systems inventory and open ports

10 Data backup procedures and system logs

BizTech **Quick Poll**

According to readers, slightly more than half of companies polled audit their IT systems, while the rest say it's not necessary, on their radar and not in their budget.

How does your company handle IT audits of its computer systems and internal access controls?

32%	We conduct it internally.
23%	We use an outside auditor.
20%	We do not feel it's necessary.
17%	We have not done one yet, but it's on our radar.
6%	Don't know.
3%	We do not have the funds or expertise.

Source: CDW poll of 281 BizTech *readers*

Outsourcing vs. In-house IT Audits

Percentage of IT audit work outsourced

- **10%** of organizations outsource 100% of their IT audit work
- **6%** outsource between 25% and 50% of their IT audit work
- **31.9%** outsource some of their IT audit work
- **41.8%** do not outsource any of their IT audit work

Strategy for the next three years

- **20.3%** of organizations plan to increase their IT audit outsourcing
- **58.7%** plan no changes to the amount of IT audit outsourcing they do
- **18.7%** plan to decrease their IT audit outsourcing

Source: Institute of Internal Auditors' 2005–2006
Global Audit Information Network annual benchmarking study

[Related Articles]

- Small but Strong
- The Right Switch for the Job
- Windows Vista Comes of Age
- Helping the Help Desk
- Reducing Costs With Microsoft Infrastructure Optimization
- Citrix NetScaler 9
- Be the Driver, Not the Driven
- Mix It Up
- Uncommonly Parallel
- Practice What You Preach

COMMENTS

From: Sara, Manchester

Just a note that the site referenced above, www.iso-17799.com, has now relocated to http://www.27000.mobi