

# most significant bits

News and Information For High-Tech Professionals

Published by Pocket Protector Press™

A division of Stout Systems



Spring 2007

## In This Issue

### Celebrating Ten Years!

Stout Systems celebrated its tenth anniversary.

### Every Audit, Every Time

Passing those pesky audits and reducing the associated costs. It can be done!

### Recent News

Stout Systems welcomes new employees Ryan Guttridge and Jean Musinski (Senior Software Engineer Consultants), Linda Reiher (Senior QA Software Engineer Consultant) and Michael Clark (Senior Systems Consultant).

### Job Openings

Check out current permanent and contract openings on our Web site StoutSystems.com.

### Current Candidates

A sampling of candidates we represent is available on StoutSystems.com.

### Subscribe To Our Newsletter

If you would like to receive this newsletter directly at your desk or in-box, send a note to [info@stoutsystems.com](mailto:info@stoutsystems.com) providing your subscription info (e-mail or ground mail address).

### Call us:

(734) 663-0877

## Always learning...

# Celebrating Ten Years!

by John Stout

**I**n May, Stout Systems celebrated its tenth anniversary.

I began my career in the software business in the late 1970s, working for a variety of employers including one of the Big Three, a major university, large agencies and small startups. These employers represented a variety of businesses that included manufacturing, electronic publishing, aerospace, warehouse systems and computer games (still my sentimental favorite job). Not one of those jobs was a waste, and every one provided new opportunities to grow not only technically but also in my knowledge of the business world.

During those years, I experienced about everything one could go through as an employee and manager. The best environments I worked were those that maintained an entrepreneurial spirit, where each individual had a stake in what went on in the company on a daily basis. That lesson stayed with me and I dedicated myself to create a own business with the same spirit.

In the late 1980s, I “hung out a shingle” and started a software consulting business which became a full-time job and grew throughout the early 1990s. In those early years, never did I imagine having to learn the ins and outs of accounting, legal, human resources, insurance, purchasing, marketing and public relations. I found that in order to succeed, I had to take responsibility for every aspect of running and growing a business.



One of the first things I had to confront and learn were contractual matters, both in terms of dealing with customer contracts but also in the hiring of partner vendors. A note to those considering a consulting career: you’ll have to learn about legal, because many customers will want you to provide a contract, rather than have their corporate counsel draw one up.

With the increasing demands of an expanding software and IT industry it became obvious by the mid 1990s that the workload was going to require a support staff of highly qualified administrative and technical people. So I began to add employees. Along with meeting a regular payroll, that necessitated learning all about taxes, unemployment, workers compensation and other types of insurance. It also required creating an employee handbook and developing a workable benefits plan.

Fortunately, having been through many types of employment experiences, I was able to identify and retain the best practices.

*continued on page 4*

## Every Audit, Every Time

By Luis Vigil, CISA

**A**udit mainly concerns itself with two things: are controls in place and are they effective? To that end, it is necessary for corporations to go through an audit or two—or more. It seems as though there is always a series of audits for one methodology other. That is, if the need is for Sarbanes-Oxley Act (SOX) compliance then a SOX audit is necessary. If the need is for an Information Technology Infrastructure Library (ITIL) assessment then an ITIL or ISO 20000 audit is necessary. The list is endless and it happens again year after year.

The typical approach is to have the same organizations and departments respond to multiple audits on an ad hoc basis. When the internal auditor shows up to do a SOX audit, IT organizations trot out the system administrators and consume valuable resources answering requests for logs, reports and documentation. Then the external auditor shows up and it starts all over again. Then the ISO auditor comes in. Then it happens again next year.

As corporations grow larger, the need to establish controls and audit their effectiveness increases; however, there are many different audits conducted and many are redundant. Not only are security or business controls audited but also conformance to methodologies such as CMMI and ITIL. The paperwork and documentation is daunting.

### Global Solution

Ultimately, the way to streamline the audit process is to apply a global solution. This entails implementing a self-assessing, self-documenting process that maintains audit questions and responses for the variety of audit types required for the entire organization.

- **Benefit 1:** Pass every audit, every time. Minimize the effort. Organize audit information so that an auditor can access read-only information relevant to the audit, thus

freeing critical resources from mundane audit tasks.

- **Benefit 2:** Get organized and deal with audit issues and controls proactively, thereby demonstrating to internal and external auditors that controls are in place and effective. The organized presentation of information relevant to an audit will demonstrate that controls are reviewed and that the organization is proactively creating a controlled environment.
- **Benefit 3:** Reduce the number of times an audit question is answered. Often the same question is asked over and over by every auditor that comes through the door. Answer the question once—and once and for all.

### How to Implement a Global Solution

1. Allocate a budget for creating an audit solution.

Okay, let's face it. Audits cost money. It costs to pay an auditor from an audit organization. It costs to tie up internal resources performing an audit. There are costs associated with remediation of findings and managing the remediation. There are also emotional costs to the arguments about findings and the management pressure to correct findings—not to mention the stress placed upon the organization by diverting resources to answer audit findings. It is better to budget these costs into a process that ensures smooth delivery of audit requirements in a pre-defined self-assessing, self-documenting audit process. This approach is best implemented as a formal project and then maintained as an ongoing process.

2. Create a documentation library.

Create a library for all the documentation, logs and reports generated by IT to support an audit. Ideally, the library is referenced via an audit document that is housed within the library. Different roles within the organization will require different levels of access to the library, but there can only be one place for all the documentation—and this is it.

3. Control the documentation that is placed in the library.

Depending on the size of the corporation, use as many Technical Writer/Librarians (TW/L) as necessary to manage the audit and compliance documentation. As an

### What is the Sarbanes-Oxley Act?

The Sarbanes-Oxley Act of 2002 is also known as the Public Company Accounting Reform and Investor Protection Act of 2002. It was passed primarily in response to scandals like the one in which WorldCom revealed that it had overstated its earnings by more than \$7.2 billion, primarily by using improper accounting techniques. One of the key provisions of the bill requires that public companies evaluate and disclose the effectiveness of the internal controls in place to monitor financial reporting. Hence SOX audits.

### What is ITIL?

The Information Technology Infrastructure Library outlines management procedures that help businesses achieve high financial quality and value in IT operations. The ITIL framework includes monitoring service support, the service desk, incident management, problem management, configuration management, change management and so forth.

example, the TW/L will draft policies and procedures, follow through on obtaining management authorization, manage the storage (official copy), and review schedules for the documentation. The TW/L is the only person who can place a document in the library. The TW/L manages the schedule for updates to documents stored in the repository and ensures that notification is mailed to the appropriate personnel. Updates are scheduled such that spikes of activity do not occur. The TW/L is the change manager and gate keeper for the documentation library.

#### 4. Standardize the audit questions.

Although each methodology asks different questions, there are many similarities to the questions. Standardizing the questions makes it possible to answer a question only once. Questions like, “Do you have a security policy,” “Is a security policy in place,” “Is a security policy in place that addresses employee conduct,” can all be put into a standard “Do you have a security policy?” slot. This is a complex task that requires the participation of a number of departments. Internal audit will be very helpful in this area if they can be engaged.

#### 5. Create a hierarchy of audit questions.

Many find that after they answer one audit question there is another lurking around the corner. This stems from the activity of measuring maturity at the same time as compliance. An example would be, “Do you have a policy,” which is immediately followed by, “Do you review the policy periodically,” “Do you have a record of the review,” and, “Does management sign off on the review?” Therefore, it is best to create a hierarchy of questions that key on the fact that the previous one has to be met before the next one can be completed. This will also accommodate the questions that have more detail than others. It is best to handle the methodology with the most detail first.

Once the questions have been standardized, label each with the appropriate methodologies. For example, “Do you have a Security policy,” could be asked by each of the following: SOX, CobiT, ITIL, ISO 20000 and CMMI. This will make it possible to sort on any one methodology and determine either the degree of compliance or the level of maturity for each of the methodologies. The advantage is that each question is answered once but applied universally.

#### 6. Manage logs and reports electronically—and, if possible, automatically.

As more and more detail becomes necessary to demonstrate controls, evidence such as system logs and reports are required. An example of a common log is “failed access attempts.” Typically, this is a large report and grows larger at the beginning of the period when users have had to change their passwords. The usual requirement

is for the log to be reviewed; some attempts may require investigation and some logs may require management review and evidence that action was taken. Assume that this is located under the hierarchy of security policy *review failed access attempts*. Create a link under the evidence column to these softcopy logs by creating softcopy records. For example, create a standard spreadsheet template for these kinds of logs, load the system log, and automatically add a header and comments field. Include a *management review* field. Review using data filters, add comments and “sign” the header. Store the logs in the document library and the TW/L keeps track of missing logs.

#### 7. Store information concerning movement of employees in the document library.

Typically, information concerning employees is sensitive. However, in order for security, system and network administrators to maintain accurate access control lists (ACLs), they must have access to information concerning the movement of employees. Therefore, a list of new employees, employees who have changed jobs/locations and those no longer with the company can be loaded in the document library periodically. Additionally, a list of current employees will aid in the access verification process. Access can be granted to those who need access to the records to accomplish their jobs. It is not necessary to add information such as the reason for leaving the company. Security, system and network administrators need to review the list against their ACLs periodically and send the results of their review to the TW/L. In order to facilitate this task and to demonstrate effective controls either a unique employee identifier or a cross-reference table with employee name and user account is required.

## Summary

Audits cost money. Spend the money up front to organize audit documentation and create a controlled process for collecting and storing evidence instead of spending it “on demand” as part of countless audits. Minimize manual effort and time-consuming tasks. Stay ahead and reduce the audit headache—but definitely pass the audit.

It may still be necessary to leave one minor area unmanaged, such as an unsigned log, just to allow the auditor to get his “finding” and avoid prolonged and painfully continuous reviews. Some auditors will deny the need for doing this; others will swear to it.

The above are just some of the examples that can be incorporated into an organized approach. Others are just a brainstorm away.

**Luis Vigil** has 30 years’ experience in IT, is CISA certified, member of the Detroit Chapter of ISACA and has audited systems worldwide.

*continued from page 1*

Some of these include:

- Don't make business decisions based on what you read in the newspapers.
- You'll succeed based more on who you hire not what methodology you use.
- Service, not cost, counts most.

For these first ten years, I want to thank our dedicated staff. Almost 50% of our staff has been working with me for that entire decade. That says a lot about our dedication and success as a team. We have continued to grow in the face of industry and business climate changes, which means that we are definitely doing something right together.

I would be remiss if I did not also thank our friends who provide excellent business advice time and again. Some of the best advice we received came from people who at one time experienced major business setbacks and challenges and then who recovered dramatically.

Most importantly, I want to thank all of our customers. Many have been with us for all ten of these years, and we appreciate their continued business very much. Some of our original customers did not survive the economic downturn of the early 2000s, but the vast majority did and are now even stronger and more vital.

We look forward the next ten years and beyond!

**John W. Stout** is the founder and president of Stout Systems Development. He has nearly thirty years' experience in the software industry. He is also sought after as a technology speaker, presenting sessions at developer conferences and user groups.



ADDRESS SERVICE REQUESTED

Presorted Standard  
US Postage Paid  
Permit #187  
Ann Arbor MI

In This Issue:

- Celebrating Ten Years!
- Every Audit, Every Time