

# MANAGING IT COMPLIANCE: SUSTAINABILITY AND SIMPLICITY FOR FUTURE AUDITS

During the short window before the next internal control audit, IT organizations should seize the opportunity to adopt sustainable IT compliance strategies.

## SIMPLICITY FOR FUTURE AUDITS

MARV TSEU

**F**or most IT organizations, meeting first-year Sarbanes-Oxley Act requirements was a trial by fire. By throwing bodies, resources, and money at the challenge, many IT organizations completed their first internal control audits through brute force. As companies plan for future audits, significant challenges still loom. First, IT organizations must manage and test a mountain of IT controls established during the first audit. In addition, the current compliance process is expensive and resource-intensive, and has detracted from day-to-day operations and core business activities. Finally, the first round of internal control audits uncovered

several serious, material deficiencies that most companies must immediately address.

Based upon these challenges, virtually every company is looking for ways to make their next audit easier and require fewer resources—all while minimizing the risk of exposing additional internal control deficiencies or weaknesses. As companies plan for their next audits, they should incorporate sustainable IT compliance tools and practices within their everyday operations. By adopting sustainable compliance strategies, IT organizations will more effectively meet ongoing compliance requirements while providing strategic benefits to the IT organization.

### Sarbanes-Oxley year one

Nearly every public company experienced unexpected turbulence during the first Sarbanes-Oxley filing. In fact, these challenges often manifested themselves in the overall business. A recent survey found that 94 percent of executives attributed their companies' compliance deficiencies to IT.<sup>1</sup> Most IT organizations were not prepared for the onslaught of evolving controls that required

*As President and CEO, MARV TSEU brings to Active Reasoning more than 30 years of experience founding, developing, and leading technology companies. As CEO and co-founder of SiteSmith, a provider of high-performance, mission-critical Internet site management services, Marv led the growth of the company from 11 employees in 1999 to 400 employees and \$20M in revenues a year later, culminating in a \$1.4 billion acquisition. Previously, he helped lead Plantronics' leveraged buyout and subsequent IPO. He held various positions at Plantronics including Vice President of Sales and Marketing, and President of subsidiary Walker Equipment Company, and today serves as Plantronics' Chairman of the Board. Marv holds a B.A. in economics from Stanford University.*

significant manual testing. In an uncertain compliance environment, internal auditors and IT organizations played it “better safe than sorry” and created an overabundance of controls (and extra work) to ensure success during year one.

The result? With a lot of work, money, and sweat, most IT organizations got through their first audits successfully. As companies plan ahead, no one wants a repeat performance of year one. As a result, many IT organizations recognize that their compliance programs require significant adjustments before the next audit.

Fortunately, most IT organizations learned a lot from their first experiences and have adequate time to make the required changes. While it may have seemed haphazard, the initial compliance process produced a consistent set of challenges for nearly every IT organization. Identifying, understanding, and addressing these common challenges will become the foundation for creating a sustainable IT compliance program. Since the yearly compliance cycle moves rapidly and has many interdependencies, companies should identify these challenges early. In doing so, IT organizations will better understand how to incorporate some of the recommendations outlined in this article.

**Lessons learned from the first audit.**

After the first internal control audit, every IT organization should take time to review the milestones, challenges, and outcomes

**COMPANIES THAT ESTABLISHED UNNECESSARY CONTROLS WILL NOW BE REQUIRED TO SPEND VALUABLE TIME AND RESOURCES TO TEST AND MAINTAIN THEM FOR FUTURE AUDITS.**

from the first compliance experience. Most likely, your experience is shared by other companies. Your first clue that the compliance process would not be a cakewalk started when you had to identify your IT controls. How many controls are necessary? What systems and applications are considered material or “in scope” of the audit? In the absence of proper guidelines and out of fear of flunking an audit, most IT organizations created an overabundance of controls in order to be “better safe than sorry.”

Unfortunately, all of these controls require ongoing testing and management.

For example, suppose you established a valid control that states, “Direct access to production databases should be restricted to authorized database administrators, and all access should be regularly audited.” This control would require ongoing testing to ensure that the control is effective and being followed. Imagine the tremendous work required to manage over 100 controls like this.

Companies that established unnecessary controls will now be required to spend valuable time and resources to test and maintain them for future audits. With all of the resources and distractions associated with the first internal control audit, virtually every IT organization is committed to reducing the waistline of their IT controls.

After the dust settled from the first internal control audits, auditors discovered a common set of issues that plagued most IT organizations. These issues were primarily associated with weak change and direct access controls. If these control deficiencies are not adequately addressed prior to the next audit, they have the potential of becoming material weaknesses, which can dangerously affect a company’s final financial filing. Since IT organizations do not want to be responsible for a material weakness that affects the business, everyone is scrambling to plug the holes in their controls.

**Implementing a sustainable compliance program**

Compliance is not going away. Every year, companies will be required to repeat the compliance process by testing and reporting the effectiveness of their IT controls. Companies want to avoid repeating the challenging and work-intensive process from the first year. So, how do you manage compliance rather than let it manage you? The answer is to implement tools and processes for a sustainable compliance program. Most importantly, sustainable IT compliance should deliver strategic benefits to the IT organization—rather than create a lot of needless work. A sustainable compliance program should incorporate the following four areas, which will be explored in greater detail throughout this article:

- automating the IT control testing process;

- closing the loop in the change management process;
- managing and minimizing the list of IT controls; and
- tackling the most common IT control gaps.

**Automating compliance testing.** In a nutshell, Section 404 compliance is all about proving that “you did what you said you were going to do” through a process of testing and reporting. During the first audit, most companies “threw bodies” at the compliance problem to manually test, validate, and report the effectiveness of their IT controls. These manual processes required excessive resources and kept IT organizations from focusing on their primary IT activities.

For the next audit, automated testing and reporting will be a requirement for most companies. If you are still unsure about compliance automation, remember the following rule of thumb: the more manual controls used, the more testing will be required during the external audit. Manual controls are a cause for concern for the auditor because they are often less accurate and effective than automated controls. Taking people out of the testing process ultimately reduces errors and improves the quality and accuracy of the testing. Often, auditors will test the automated control once and retest the configuration of the control during subsequent audits.

Most importantly, by taking people-intensive resources out of the testing process through automation, companies will reduce auditing expenses and reallocate resources to higher-value tasks that are strategic to the IT organization.

So, which controls should be automated? The answer is relatively straightforward. Focus on the manual, time-intensive IT controls that require forensic data from systems and applications. For example, a control that is currently validated through interviewing, having people fill out forms, or walking through the data center with a clipboard is not a good candidate for automation. A control that is validated by logging on to servers, reviewing change requests, or sifting through security logs is a prime candidate. Controls that fit this bill include auditing direct access to systems and databases and ensuring that changes made to mate-

rial systems are following the prescribed change control process.

**Automating change control and direct access testing.** Automating testing for direct access and change management requires that IT organiza-

tions first gain insight into “who is doing what” to material systems and applications. More specifically, IT organizations should collect change activity data on activities that are specific to a defined control point, such as:

- direct access—people logging onto financial servers or databases;
- databases—changes made to databases housing financial data;
- files and configurations—file or configuration changes supporting financial applications; and
- Active Directory or LDAP systems—user access permissions and modifications to financial systems.

During the first internal control audit, many IT organizations collected this change activity data by manually sifting through security, operating system, and database logs, as well as change request systems. Using an automated tool to detect and report change activity data in a relevant format saves a lot of time, headaches, and resources. Depending upon the control, internal auditors should review changes and direct access by user, application, or device, or within a specific time window.

The final—and most important—step in this process is to validate the change or direct access activity. Does the activity (e.g., a configuration file change to a financial application) adhere to the control or process (e.g., obtaining an approved change request before making the change)? Was the change activity completed as planned? How many changes went outside of the change management process? Through this automated process, IT organizations will always be aware of unauthorized changes and direct access and will be able to take corrective action before the external auditor arrives.

**Closing the loop on the change management process.** Many companies have invested in change management systems

**FOCUS ON THE MANUAL, TIME-INTENSIVE IT CONTROLS THAT REQUIRE FORENSIC DATA FROM SYSTEMS AND APPLICATIONS.**

that incorporate tools and business processes for identifying, planning, assessing, approving, and assigning a change. This process ensures that change activities are communicated and coordinated, and have a minimal impact on the overall business.

Unfortunately, today's change management systems cannot validate change activities once an approved change request has been assigned to an individual. Did the change actually get completed? Is there a change request associated with an observed change? While change management deals with "what is supposed to happen," audit efforts are all focused on "what really did happen."

Closed-loop change management is an audit strategy that combines "what was supposed to happen" with "what really did happen." By leveraging and extending the capabilities of the change management system, every change becomes a test of the change control process to catch unauthorized changes and direct access and to report that approved changes were actually completed. By comparing detected changes with approved change requests from the change management system, a closed-loop solution immediately reports unauthorized activities, including the individual associated with the change. Once an individual completes a change, the change management system will then report all of the activities associated with the approved change request.

**Taking control of IT controls.** Under pressure during their first internal control audits, many IT organizations implemented more controls than were really necessary. As discussed previously, excessive controls ultimately translate into more work and effort during future audits. Before the next audit, most IT organizations should reassess their lists of controls.

So, which controls are absolutely necessary? IT organizations should identify the minimum number of controls that ensures the maximum integrity of financial systems, applications, and data. When reviewing their lists of controls, IT organizations should ask themselves the following question: does the control have a direct effect on the financial reporting? For example, if you are a lumber company and do not conduct e-commerce via the Internet, an open port on a firewall should not be a major cause

for concern. However, if you are an eBay or PayPal, this control becomes critical.

The company's external auditor can tell the company which controls it considers absolutely necessary. However, IT organizations should not hesitate to push back and discuss questionable controls with their auditor. If you can't establish a direct relationship between the control and the financial reporting, tell your auditor that you want to talk. By reviewing and reducing the list of controls, you create less work for yourself, while reducing external auditing expenses.

### Tackling the most common IT control deficiencies

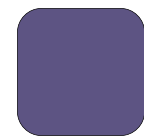
Following the first internal control audit, many IT organizations found themselves joining the ranks of companies with common IT control deficiencies. The short list of common IT control deficiencies identified by the major audit firms includes:

- lack of access controls;
- excessive access to systems and databases;
- improper change management;
- inadequate segregation of duties; and
- lack of a self-assessment process.

When approaching the next audit, IT organizations should focus on these common gaps. With the first major audit cycle under their belt, the auditors know where to focus their primary efforts.

**Lack of access controls and excessive access.** Most financial applications have adequate access controls at the application layer. For example, a PeopleSoft general ledger application is equipped with password protections to ensure that only authorized individuals can make changes through the application interface. However, companies should be equally concerned with access outside of the application, such as a person logging into a server to access critical data or files. Common causes for this type of control gap include:

- job changes—inadequate controls in place to delete or change access when an individual leaves a job or changes job responsibilities;
- administrator passwords—poor administration and management of administrator passwords; and



**IF YOU CAN'T ESTABLISH A DIRECT RELATIONSHIP BETWEEN THE CONTROL AND THE FINANCIAL REPORTING, TELL YOUR AUDITOR THAT YOU WANT TO TALK.**

- inappropriate approval of access changes—changes in access permissions for individuals, groups, or roles within the IT organization that do not obtain adequate approval.

A common access control gap cited by the auditing community was excessive access to databases and systems. Many users do not require access beyond the front-end of the application. Auditors frequently found database administrators accessing financial databases without a corresponding reason or approved change request.

Auditors also detected weak management of administrator access privileges. This type of access is managed through “administrator” passwords, which are usually granted on a temporary basis and should expire or change after a certain period of time. Many auditors reported poor management and abuse of administrator access simply because the passwords never changed. Similarly, these passwords were often managed without proper segregation of duties (e.g., a system administrator managing all of the password accounts).

**Weak change management.** Change management has always been a sticky subject for most IT organizations. Unauthorized changes and direct access are often the primary culprits of unplanned downtime. With the Sarbanes-Oxley Act in place, unauthorized changes and poor change management now take on an additional risk if they are the cause of a material weakness.

Some common change management issues include:

- *Changes occurring outside of the change process.* Some companies estimate that many changes still occur within their environments without the appropriate approvals from the change management process.
- *Change control processes not in place.* During the first round of internal control audits, many companies were forced to document their change management procedures for the first time.
- *Inability to validate whether changes were actually completed.* Most IT organizations have a limited ability to validate planned changes

and verify whether the work was actually completed.

**Inadequate segregation of duties.** Segregation of duties is a basic but frequently overlooked internal control. During the initial internal control audits, auditors often found that individuals had control over two or more phases of a transaction or operation. Responsibilities should be assigned to crosscheck duties. For example, a helpdesk administrator should not have administrator access to the network. Ultimately, proper segregation of duties ensures that errors or irregularities are prevented or detected on a timely basis by members of the IT organization during the normal course of business.

**Lack of a self-assessment process.** IT organizations should test their controls at least quarterly. The goal of the testing process is to identify control gaps early in the compliance process and produce the necessary documentation to aid auditors during the external audit. Unfortunately, with limited resources and time, most IT organizations have not found the time to establish a regular testing program.

Like excessive manual controls, a lack of a self-assessment process is a concern for auditors. During the course of the self-assessment process, reports will attest to the effectiveness of a control throughout the year. Without this documentation, auditors will naturally require more extensive testing to feel comfortable with each control. Automated tools and processes will help reduce the workload associated with the self-assessment process.

### Getting something out of compliance

Compliance undoubtedly is costing most companies significant money, time, and resources. If you’re going to be putting a lot into this initiative, shouldn’t you get something out of it? Believe it or not, compliance has a silver lining. Through the hard work to meet the Sarbanes-Oxley Act’s requirements, your IT organization will achieve several tangible benefits that bring strategic value to your company. These include:

- improved IT operations;
- reduced costs and reallocated resources; and
- increased overall compliance.

**LIKE EXCESSIVE MANUAL CONTROLS, A LACK OF A SELF-ASSESSMENT PROCESS IS A CONCERN FOR AUDITORS.**

**Improved IT operations.** By establishing effective IT controls that are tested year-round, IT organizations will streamline core IT operations processes through improved change management, direct access controls, and security. For example, strengthening the change control process will reduce unauthorized activities and reduce unplanned downtime.

Most importantly, the compliance process increases accountability within the IT organization. Since compliance places the spotlight on “who did what,” everyone within the IT organization is now cognizant of how their actions and activities directly affect the overall business.

**Reduced costs and reallocated resources.** By leveraging automated compliance tools, IT organizations will dramatically cut their audit and compliance costs. These costs—and the individual resources associated with them—can be reallocated back to the business for more strategic initiatives.

**Increased overall compliance.** Compliance is not only about the Sarbanes-Oxley Act. There are host of other general and industry-specific compliance requirements that companies must meet. Strengthening core IT controls for change management and direct access also strengthens your hand with other health, financial, and federal compliance requirements, for example.

## Conclusion

During the short window before the next internal control audit, IT organizations

should seize the opportunity to adopt sustainable IT compliance strategies. These strategies reduce compliance costs and resources while minimizing compliance risks. First, by incorporating automated IT control testing for change management and direct access, companies will reduce the compliance workload and improve the accuracy of financial reporting. By extending change management systems to automatically audit every change detected within the infrastructure, companies will immediately catch and stop unauthorized changes—a key concern for auditors. Next, by reducing the growing list of controls to those that are absolutely necessary, companies will better manage their testing processes. Finally, by focusing on the common control gaps identified by external auditors, IT organizations will avoid pitfalls during the next audit.

Sustainable IT compliance is also an opportunity to bring competitive benefits to the company. Remember, every public company is facing the same compliance challenges. Ultimately, the company that does compliance right will immediately gain a competitive advantage. The company that gets it wrong and fails to adopt a sustainable compliance strategy wastes time, resources, money, and potentially public prestige if its material weaknesses result in a restatement of earnings. ■

---

### NOTE

<sup>1</sup> “Sarbox and IT: How Bad Can Things Get?” *CFO IT* (Summer 2005), available online at [www.cfo.com/article.cfm/4077489](http://www.cfo.com/article.cfm/4077489) (accessed August 2005).