ecora

WHITE PAPER

Avoiding Costly Audit Deficiencies

Using a pre-audit assessment to fix problems before your auditor shows up

Compliance pressures are growing. In the past, ensuring compliance was seen primarily as a way to protect an organization in the event of an attack, whether from external forces, such as hackers mining for customer data, or from sources closer to home, such as employees or consultants who wanted to manipulate data for personal gain.

Today, however, the need for continuous compliance is driven by more than security threats. Organizations are confronted by government and industry regulations and requirements, legal restrictions, concerns about consumer fraud and privacy, and even mandates from investors and business partners. The one common thread in all these factors: the requirement to remain continuously in compliance.

With the growing number of compliance mandates being enacted and the complexities of maintaining continuous compliance, organizations need to understand the challenge and make the commitment to meeting it. To accomplish this, organizations have to move toward viewing compliance as an integrated business process, using IT best practices and an IT governance model that aligns the IT organization with the business strategy. For most organizations, the audit process continues to reveal deficiencies—from a lack of access controls to improper change management procedures, from inadequate segregation of data to a lack of self-assessment processes.

How can your organization eliminate costly deficiencies like these prior to an audit? In this whitepaper, we'll discuss ways your organization can leverage a pre-audit assessment to identify compliance gaps, generate effective reports for documenting controls and proving compliance, test the operational and design effectiveness of your controls, and use automated tools to determine control weaknesses in your environment.

Begin by Leveraging Automation

As the gap continues to grow between compliance requirements and stagnant—or shrinking—IT resources, organizations must leverage the benefits of automation, particularly when it comes to the data collection and reporting necessary for documenting IT controls and policies. In fact, a recent *InformationWeek* study indicated that "organizations with the fewest compliance problems are spending 9 percent more to automate audit functions and eleven percent less on contractors and outside services." (*InformationWeek*, December 4, 2006)

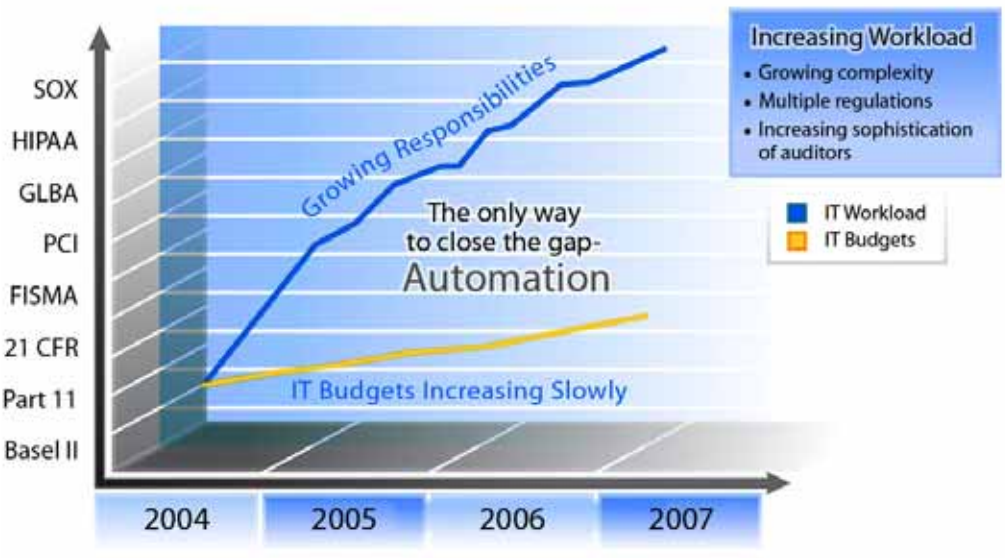

Figure 1. Increasing Gap between IT Budgets and Workload.

"Automating IT security functions, not consultants or services, along with frequent auditing of data security, improves compliance, an IT Policy Compliance Group study shows…Companies most likely to successfully navigate today's regulatory environment need to automate IT security functions rather than blow their budgets on pricey consultants or services, and they need to do more frequent auditing of the systems and data security."

—Larry Greenemeier
InformationWeek

Understand the Regulations and Requirements

One of the main reasons an audit may reveal deficiencies in the IT infrastructure is a general lack of understanding about the regulatory requirements an organization faces. Even when a company feels adequately prepared, it can still be difficult to know exactly how specific requirements will be interpreted by auditors and which technologies will actually improve compliance efforts.

It is important for you to increase your understanding of the regulatory requirements your organizations faces. One way to accomplish this is by tapping into the knowledge of others within your organization, including legal and security experts, as well as anyone who engages with government or regulatory agencies. Make sure someone on your staff monitors new proposals as they wind their way through Congress. Two proposals—the Notification of Risk to Personal Data Act (S 239) and Personal Data Privacy Act and the Cyber Security Enhancement and Consumer Data Protection Act (S 495)—could both lead to strict penalties and even possible jail time for those who fail to report security breaches.

It is also important to pay attention to the laws in your own state and any states where you conduct business. Minnesota, for example, has made compliance with Payment Card Industry Data Security Standards (PCI DSS) a state law, and it is likely that other states will follow suit. By legislating PCI DSS at the state level, states will have a statute providing the recourse to sue companies that have breaches involving cardholder data.

Prepare for an Audit with a Pre-Audit Assessment

By conducting a pre-audit assessment, you can identify any deficiencies and gaps in your environment before auditors do. You'll also benefit from having time to remediate any deficiencies or gaps that are discovered prior to the audit.

As an added benefit, a pre-audit assessment allows you and your management team to evaluate internal controls and security procedures—a process that should be scheduled at regular intervals and can be streamlined through an internal assessment process.

A pre-audit assessment typically begins with a complete inventory of all areas where data may be transmitted or stored, including:

- Routers, switches, firewalls, IDS/IPS, wireless
- Servers, PCs, mainframes, PDAs
- Hard disks, printouts, backup tapes, audio recordings, vendors and third parties and their sub-servicers
- Load balancer(s), click tracker, middleware, SSL accelerator, TOE card, webserver, application server, database server
- IVR, call center "OB" (observation) capture systems
- Temp files, C:\ drives, flash drives, file server with "Everyone" access

Compiling this inventory is critical. Knowing all the systems and devices in your environment and providing accurate documentation to your auditor will make the entire audit process go more smoothly. An audit will include a sampling of your systems and devices, across all physical locations, and there is nothing worse than your auditor asking for information about a server or other device that you didn't know existed—particularly if it turns out not to meet the operational standards your organization has established.

An inventory also reveals the location of all sensitive and confidential data, including electronic protected health information, social security numbers, card holder data, as well as all those involved with your organization who use customer data, such as local and remote staff, consultants, business partners, and regulators. Keep in mind that compliance requirements extend to anyone who interfaces with your organization and sensitive or confidential data.

During the pre-audit assessment, you should also review the controls currently implemented within your computing environment, including access controls, password policies, policies and procedures, and change and configuration management processes.

Five Keys to a Successful Control Self Assessment (CSA)

1. Automate the IT control process. By eliminating the "human" element of compliance, you can ensure consistency and preparedness, regardless of when an audit takes place. Many auditors themselves are taking advantage of the automated tools available, increasing their awareness of the capabilities automated tools can offer.

2. Evaluate and adjust. Compliance must be process driven, and as with any business process, the effectiveness of IT controls and compliance initiatives must be evaluated regularly to ensure they continue to align with business objectives and strategies.

3. View compliance as an opportunity. Think of compliance efforts—and even audits—as opportunities to improve core IT and operational processes and affect positive change in your environment. Look at an audit as an opportunity to make IT controls and operations more effective, as well as to validate security controls and pinpoint vulnerabilities in your infrastructure.

4. Manage and document your controls. There is a direct relationship between IT controls and business processes. You should constantly evaluate which controls are material to business systems, and anticipate and document change; as business requirements change, for example, systems change, controls change, and processes change.

5. Don't reinvent the wheel. There are multiple compliance requirements, and analysts predict the number of requirements will continue to grow. Use existing standards like ITIL and COBIT as benchmarks, and then leverage processes and controls across all compliance mandates to satisfy multiple requirements.

Finally, you should document and resolve all the gaps between internal and external compliance requirements and the actual state of compliance recorded in the pre-audit assessment. Demonstrating to your auditor that problems identified during a pre-audit assessment have been remediated will help focus the audit process.

There is one particularly important benefit of completing a pre-audit assessment. Many compliance regulations are still in their very early stages, and many of their requirements may be open to interpretation. If an audit reveals a deficiency in your IT infrastructure and you have a compliance process in place that includes periodic monitoring, such as a pre-audit assessment which is complete and up to date, you may be able to prove to your auditor that you had already identified the problem and have a process in place to correct it. In fact, under the Federal Sentencing Guidelines Act, if you have a control process in place but make a mistake anyway, the penalties are far less severe than if the reverse was true. This is why formal internal assessment procedures are invaluable. If you know your position and you're doing something to rectify it, you are likely to face fewer repercussions for a deficiency.

You may also face fewer penalties if you let your auditor know ahead of time that your pre-audit assessment efforts have revealed a problem. Not advising them in advance will only make their own forensic efforts more difficult and time consuming and, in the case of PCI for example, may impact consumers and will definitely diminish your negotiating position. Again, negotiation may be possible—and will be more effective—if you have a repetitive monitoring process in place.

Leverage the results of your pre-audit assessment to show your auditors what you're doing well. For example, you should share security and control improvements you've made since your last audit or procedures you've implemented that your competitors might not have considered. Highlight the depth of your security defenses—or use of other compensating controls—to show how overall security and control efforts can enable you to overcome individual deficiencies.

Completing a pre-audit assessment and following these steps will demonstrate your organization's commitment to ensuring continuous compliance.

Pinpointing—and Remediating—Deficiencies before an Audit Begins

Ecora provides software and services that allow organizations to implement sustainable, automated IT compliance programs.

One such Ecora service is the Ecora Pre-audit Assessment. Typically a two- to three-day engagement, this service collects configuration data from across operating systems, database management systems, directories, applications, mail servers, network devices, and firewalls, and reviews the controls currently implemented within your computing environment. The Pre-audit Assessment also includes automated reports that compare the data against any of the major compliance requirements. The process identifies any gaps between the environment and the standards, and provides actionable information to remediate deficiencies.

To learn how Ecora's Pre-audit Assessment or other Ecora software and services can help you automate detailed reporting for regulatory compliance audits and enabling IT best practices, call 877.923.2672 or +1 603.436.1616, email sales@ecora.com, or visit us on the web at www.ecora.com.

About Ecora Software

Ecora Software provides Enterprise Configuration Visibility™ to customers worldwide, ensuring their IT infrastructures are secure, compliant and effective. Ecora is the market-proven leader in transforming enterprise-wide configuration data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's flagship solution, Auditor Professional,™ provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for more than 3,600 customers, including many of the Fortune 100. For more information, please visit Ecora at www.ecora.com.

ecora

2 International Drive, Suite 150 | Portsmouth, NH 03801 | p:877.92.ECORA 603.436.1616 | f:603.436.4344