



IT Director's Series

**Sustaining Sarbanes-Oxley IT Internal
Controls**

Index

Executive Overview	3
Sustaining Sarbanes-Oxley IT Internal Controls	4
Sarbanes-Oxley Overview	4
Section 302: Corporate Responsibility for Financial Reports.....	4
Section 404 -- Management Assessment of Internal Controls	5
A Brief Review of Controls over IT Systems	6
Evaluating IT Relevance.....	6
Testing Internal Controls	7
Building a Sustainable Model for IT General Controls	8
Change – The Nemesis of Sustainable Compliance.....	8
From an IT general control perspective any change needs to be managed to maintain compliance. These changes include (but are not limited to):.....	8
Change and Configuration Management	9
IT General Controls Sustainability	10
IT Controls and Automation	11
A Template for Sustainable IT General Controls.....	11
Systems Security.....	13
Configuration Management	16
Operations.....	17
Data Management	18
Summary.....	19

Executive Overview

Sarbanes-Oxley is the most comprehensive financial regulatory law in US history. It places responsibility for accurate and reliable corporate financial reporting in the hands of the CEO and CFO. It holds senior management specifically responsible for any and all shortcomings.

Senior managers are now responsible for the design, implementation, and internal assessment of internal controls for financial reporting. In today's world a significant part of those controls are embedded in the IT department.

The first (and much delayed) deadlines have come and gone. Despite the pain of meeting the deadline, many companies are now seeing the benefits of comprehensive internal examination of the processes, systems, and people involved in financial reporting systems.

Companies have now experienced what Sarbanes-Oxley means in terms of compliance. For most it was a time-consuming, intense exercise. The resources required to meet compliance deadlines exceeded most people's estimates. Big accounting firms tagged the average cost of compliance at \$7.8 million.

If you're not hearing a collective sigh of relief, it's because most executives realize that the challenge of sustaining SOX compliance will require substantial additional resources. SOX requires both annual and quarterly audits of management's assessments of internal controls. This means that internal control tests and reporting need to be on-going.

Solutions must be found and implemented that make compliance sustainable without huge investments of time and resources.

From a corporate perspective this means a wide range of institutional, process, and behavioral change must occur. In IT – in some ways – this is a more straightforward proposition. Tools are available that can automate significant parts of IT Internal controls.

This paper explores what is required for IT to build a sustainable system of IT general controls.

We provide a working model that takes the pain out of the detailed, mundane tasks associated with collecting and reporting on data that auditors require. We've taken our experience with customers and relevant research to develop some working guidelines for designing, testing, and documenting IT internal controls.

We'll also give a brief overview of the Sarbanes-Oxley law. Our focus is on IT general internal controls. This document is not intended as a Sarbanes-Oxley silver bullet. Its intent is to provide some templates that IT managers can use to build a complete sustainable IT general internal control structure.

Sustaining Sarbanes-Oxley IT Internal Controls

Sarbanes-Oxley Overview

The Sarbanes-Oxley Act of 2002 was fashioned to protect investors by requiring accuracy, reliability, and accountability of corporate disclosures. It requires companies to put in place controls to inhibit and deter financial misconduct. And it places responsibility for all this – unambiguously – in the hands of the CEO.

Failure to comply with Sarbanes-Oxley exposes senior management to possible prison time (up to 20 years), significant penalties (as much as \$5 million), or both.

Sarbanes-Oxley is one of the most complete American corporate anti-crime laws ever. It focuses on and proscribes a range of corporate misbehavior such as, altering financial statements, misleading auditors, and intimidating whistle blowers. It doles out harsh punishments and imposes fines and prison sentences for anyone who knowingly alters or destroys a record or document with the intent to obstruct an investigation.

Sarbanes-Oxley is clear on what it disallows, and sets the tone for proper corporate conduct. It does not, however, detail how to become compliant. It leaves the bulk of that decision and definition in the hands of individual businesses. This flexibility is a plus in that it provides wide latitude in compliance. However, the lack of detail has created some confusion as to what constitutes appropriate controls.

Yet, the cost associated with lack of compliance is very real. Moody's Corp. has taken negative credit action against 20% of companies it covers that reported material weaknesses in their controls.

Much of the discussion about Sarbanes-Oxley as it relates to IT focuses on two sections: 302 and 404. In addition, the Public Company Accounting Oversight Board (PCAOB) issued *Auditing Standard No. 2* which provides detailed guidance to auditors of Sarbanes-Oxley compliance.

N. B. PCAOB recently (4/15/05) acknowledged the difficulty and cost associated with 404 compliance and indicated it would be reviewing standards and issuing new guidance and perhaps reopening the rule.

Section 302: Corporate Responsibility for Financial Reports.

Sarbanes-Oxley 302 specifies that certifying officers are responsible for establishing and maintaining internal control over financial reporting.

302 requires:

- A statement that certifying officers are responsible for establishing and maintaining internal control over financial reporting.
- A statement that the certifying officers designed internal controls and provide assurance that financial reporting and financial statements were prepared using generally accepted accounting principles.
- A statement that the report discloses any changes in the company's internal control over financial reporting that have materially affected those internal controls

This section makes corporate executives clearly responsible for establishing, evaluating, and monitoring internal control over financial reporting. For most companies the IT department is crucial to achieving this goal. IT is the foundation of any system of internal control.

Section 302 Sustainability Requirements – Quarterly audits

PCAOB, in Auditing Standard No 2, states:

“The auditor should perform limited procedures quarterly to provide a basis for determining whether he or she has become aware of any material modifications that, in the auditor’s judgment, should be made to the disclosures about changes in internal control; over financial reporting in order for the certifications to be accurate and to comply with the requirements of Section 302 of the Act”

Section 404 -- Management Assessment of Internal Controls

Section 404 of Sarbanes-Oxley requires companies that file an annual report to include an internal control report that states the responsibility of management for establishing and maintaining an adequate internal controls structure and procedures for financial reporting.

Compliance with Section 404 originally became effective on June 15, 2004, for all SEC reporting companies with a market capitalization in excess of \$75 million. That was later extended to November 15, 2004. For accelerated International companies that file periodic reports with the SEC, the compliance deadline has been extended to April 15, 2006.

A company that is not an accelerated filer, including a foreign private issuer that is not an accelerated filer, will begin to be required to comply with the Section 404 requirements for its first fiscal year ending on or after July 15, 2007, following a September 15, 2005 decision from the SEC.

Section 404 is contained in 19 lines of the law. Those 19 lines have generated more ripples in the IT Industry than anything since Y2K. A significant outcome of 404 is that IT can no longer keep the technological lid on their world. Sarbanes-Oxley auditors will be delving deeply into the IT infrastructure to test validity and accuracy of IT internal controls.

There is another catch – Sarbanes-Oxley is intentionally vague and broad on what internal controls are required to meet auditing standards.

Section 404 Sustainability Requirements – Annual Audits

Compliance with Section 404 requires companies to establish an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse. This infrastructure must ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of the business processes.

Companies must assess their internal controls to ensure financial reporting is accurate and reliable. It also requires independent audits, whose auditors must report any material weakness to investors. These auditors get their guidance from the PCAOB’s Auditing Standard No. 2.

Auditing Standard No 2 is over 200 pages. It gives auditors guidance as to how to audit for SOX. Based on experience from the first round of audits, auditors are being quite conservative about what constitutes a material weakness and requiring disclosure of everything to protect themselves from regulators.

That's one reason why the PCAOB is reviewing auditing standards as they relate to Section 404 right now. However, expect strict interpretation of the law by auditors for the immediate future.

A Brief Review of Controls over IT Systems

Based on Ernst & Young data, there is a wide range in the number of processes being documented and the number of controls being documented within each process. Companies are documenting anywhere from five to 50 processes per location with two-thirds evaluating less than 25, which highlights the confusion around 404 internal controls.

It seems the PCAOB went out of their way to be as vague as possible as to what internal controls are necessary. They defaulted to:

“Internal control is not “one-size-fits-all” and the nature and extent of controls that are necessary depend, to a great extent, on the size and complexity of the company.”

Consequently, companies and auditors are both struggling to determine what an appropriate level of internal control is, and to what level must they be defined and tested.

With IT playing a fundamental role in most business processes, controls are needed over all systems. IT controls generally cover IT environments, access to systems, programs, and data, computer operations and change management. IT governance is an essential piece and contributor to overall financial governance.

Regardless which framework you select, organizations must select accounts that are material to financial reporting. This involves mapping control objectives for financial reporting to IT control objectives. This means that IT management must become intimate with and conversant with common financial concepts such as:

- Existence and occurrence – controls should address the possibility of duplicate, retransmitted, or fictitious transactions during all processing stages.
- Measurement – measurement criteria should be tailored to the requirements on the basis of relevance to financial reporting.

Many internal controls for financial reporting are IT dependent. In defining internal controls it is important to articulate the central technology components of business processes and increase the understanding between IT and business members of the Sarbanes-Oxley team. It is also critical to determine if an IT process or component is relevant to SOX compliance.

Evaluating IT Relevance

While many IT controls are essential to smooth functioning of IT itself, they may have little or no bearing on Sarbanes-Oxley compliance. To add value to Sarbanes-Oxley initiatives, IT

controls need to help meet the act's requirements. Some questions to consider when evaluating IT control relevance include:

- Is the computer processing directly or indirectly related to the timely production of financial reports?
- Is an IT process critical to the business?
- Is an IT activity connected with an important account?
- Are there known deficiencies or material weaknesses in a technology?
- Is this a high-risk computer operation?
- Is the financial application a feeder system to several system interfaces — from transaction origination to final destination — in a major general ledger account?
- Is the application characterized by: high-value and/or high-volume transactions, automated computation and reconciliation, straight-through processing, and a high volume of non-routine procedural bypasses/overrides?
- Is the application shared by many business units across the enterprise?
- Is this IT process dependent on manual controls to complete the end-to-end process?
- Is this IT process managed by a third-party outsourcer?

Questions such as these can help place relevance boundaries around your IT operations and infrastructure.

IT general controls cover a wide range of behaviors and systems at the infrastructure level. This includes program development, change management, computer operations, and access to programs and data. (For a detailed review of IT general controls see Ecora's "*Practical Guide To Sarbanes-Oxley Internal Controls*")

If you have sound IT general controls you, by definition, limit the exposure of all the controls on the other levels – especially application controls. The reason for this is that the amount of testing required at the application level diminishes if you demonstrate that controls at the network, database, and OS level are sound.

Testing Internal Controls

Remember, Sarbanes-Oxley is all about financial reporting. A company's management needs to decide which controls it depends on to detect material errors in financial statements. They need to decide which combination of controls and testing will provide the right level of assurance.

Again, there is no simple answer. Each company needs to develop a testing program that management believes in. After all the intent of Sarbanes-Oxley is to have senior management own and manage the control process – from design to implementation to assessment.

Some companies drove their compliance effort to an internally acceptable level of resource, cost, and risk. Then waited for their first audit to determine an on-going action plan.

However, the "control – test – document" model is one that will become ingrained in companies as Sarbanes-Oxley establishes itself as an on-going compliance requirement.

Building a Sustainable Model for IT General Controls

Preparing for the initial SOX audit opened the eyes of many executives to the relevance of IT to their financial information. Internal audit departments and financial management initially drove the compliance effort. However, once the scope of SOX was clearly understood, IT management became central to the compliance effort.

This involvement created a couple of interesting dynamics in the IT world; IT management was forced to understand and implement SOX requirements, and IT was put in the unfamiliar position of having independent, not-necessarily-technical auditors looking over their shoulders.

Ernst & Young estimated that 10% of first year SOX audit questions focused on IT controls. E&Y projects that will grow to 25% in year two and beyond. This places a significant burden on IT to develop processes and systems that automate their compliance efforts.

Add to that the requirement to link ongoing Section 404 monitoring effort to quarterly Section 302 reporting. (Remember, Section 302 requires quarterly evaluation and reporting of changes to internal controls that could have a material effect on financial statements). Companies – and IT departments – need to develop ways to keep the assessment of internal controls dynamic over time and cannot wait until year-end to evaluate changes.

Change – The Nemesis of Sustainable Compliance

A successful CIO once said “When things change is when they break.” He could have been speaking directly to compliance efforts -- because change moves you from compliance into non-compliance.

From an IT general control perspective any change needs to be managed to maintain compliance. These changes include (but are not limited to):

- People
 - Terminated voluntarily and otherwise
 - Role and responsibility changes – with access implications
- Sarbanes-Oxley Interpretation
- IT Internal Controls
- Financial Systems
- IT System Configurations

From an IT perspective each of these change areas needs to be addressed. It demands that IT be involved in the day to day management of SOX compliance. If your internal controls are established with appropriate tests in place **and** you have a change management system in place you are well on your way to a sustainable compliance environment.

How well you track, manage, and document changes goes a long way towards determining how consistent and relevant your compliance effort will be – and how costly in resources and productivity it is.

Change and Configuration Management

Few companies completely understand and control their infrastructure. Many can't tell you exactly how many servers are active – let alone define each server's configuration. Sarbanes-Oxley forced companies – and IT departments – to examine and define the financial related pieces of the infrastructure. In some cases it also forced the opening of IT to outside auditors for the first time.

The rationale for systematically managing and controlling changes to IT infrastructure goes far beyond Sarbanes-Oxley compliance. If such a system was in place the pain of meeting SOX requirements would be substantially less. However, the documentation and reporting from a change and configuration management system would also automatically support security, disaster recovery, and daily troubleshooting efforts.

Change and configuration management (CCM) plays a central role in IT best practices such as ITIL and COBIT. It provides accurate and current information in order to properly plan, conduct, and validate changes, which reduces downtime from planned and unplanned changes.

IT infrastructure is always changing. New services get added. Servers are added or removed. An expanding mobile, wi-fi enabled workforce demands a high level of service and requires additional security and management oversight. Unauthorized changes from external (worms, viruses, malware) and internal (Gartner says 80% of attacks come from inside) sources make security a moving target. And there is little margin for error with 24/7/365 uptime the expected standard.

In this dynamic environment it is impossible to manually track, document, and manage changes. That's where CCM comes in.

In simplest terms, CCM systems collect, archive, and report detailed system configuration data. By automating and standardizing this data, accuracy and reliability increase dramatically. There is also a dramatic decrease in resources needed to collect the data – providing almost instant ROI.

Understanding your existing systems significantly improves your planning and management of the IT infrastructure. This starts with detailed documentation. Prior to automation organizations rarely (if ever) documented IT infrastructures because system documentation could only be done manually. By the time a system was entirely documented, the process had to begin all over again to stay current. Good IT documentation lets you:

- Create "Audit-Ready" documents on demand – an essential component for SOX IT general controls.
- Detect security vulnerabilities
- Simplify server consolidation
- Understand dependencies between parts of the network
- Optimize network and system configuration

- Standardize configuration settings across all systems
- Accelerate problem resolution and troubleshooting
- Migrate to new platforms: knowing established baselines and subsequent changes is critical
- Manage and preserve system knowledge despite IT staff changes
- Speed up Disaster Recovery – limiting downtime
- Educate new staff and consultants on the organization's IT infrastructure

Even without a driver such as Sarbanes-Oxley, CCM's documentation capability and cost savings make compelling acquisition arguments.

Good change and configuration management and the resulting documentation support complete and constant change management. It can be the foundation for managing your entire IT infrastructure with value in security, standards and policy implementation, and day to day management along with compliance.

IT General Controls Sustainability

IT is indispensable to SOX compliance. It is interwoven into just about every aspect of financial reporting. So in some ways it is off mark to discuss IT as a separate compliance segment. However, IT general controls are the provenance of IT and need to be addressed with IT sensibility and tools.

While most provisions of Sarbanes-Oxley focus on financial records, it is clearly not meant to stop there. For example, during an investigation, discovery requests can be submitted to IT departments. In addition, such requests could require access to all e-mail communication or other digital information managed by IT.

IT general controls address the underlying technological infrastructure of an organization. This is where database, network, and system access is authorized, controlled and documented. The initial compliance effort in many cases established a plan and uncovered a wide range of issues that need to be addressed to build sustainability.

The good news is that the groundwork has been set and processes established around IT general internal controls. The bad news is that change is constant in most organizations.

Going forward the compliance effort will probably not be as great as year one. Yet the overall process will need to be conducted – and kept current -- during each year. Done correctly, this task requires continuous focused management.

A primary objective of sustainability is to build continuity between the team and the effort it took to meet year one objectives and the continuing process of compliance. This requires a structured effort to establish processes before responsibilities shift. Institutional learning that occurred in the first year must be captured and used productively.

The development of this on-going process will, by necessity, be managed by the Controller, Audit Group, or new compliance manager. Regardless of where the process ownership ultimately resides, IT will continue to play a central role in SOX compliance.

IT Controls and Automation

The PCAOB mandates that each year's assessment of internal controls stand on its own. This puts a premium on improving all your processes as much as possible. One way to do this is by building better controls around your IT infrastructure and automating the testing and reporting of those controls. Another is to leverage IT based controls and automation to cut down on human resources.

This is where automation can play a significant role in providing continuous compliance. With a tool such as Ecora's Auditor Professional, data collection and reporting for IT general controls can be completely automated.

A Template for Sustainable IT General Controls

As we've pointed out repeatedly, Sarbanes-Oxley is about financial reporting. When you are defining IT general controls it is to your benefit to make sure that you clearly define the systems and processes that touch your company's financial reporting universe.

In COSO there are two broad groupings of IT internal controls:

- Application Controls -- apply to business processes they support and designed within the application to prevent and detect unauthorized transactions
- General Controls -- apply to all information systems, support secure and continuous operation.

In order to construct IT general controls, functional areas can be delineated to provide a suitable template for specific controls. These include:

- Systems Security
- Configuration Management
- Data Management
- Operations

Each of these areas has multiple controls – some of them logical documented policy statements, others more concrete, data measurable processes.

For each internal control, single or multiple tests can exist to demonstrate the controls' validity. In many policy instances a copy of a written plan is an acceptable test. In other cases such as security or configuration, documented reports showing appropriate data points from a system will be required.

Ecora Auditor Professional and IT Internal Controls

Ecora Auditor Professional is configuration and change reporting software. It provides automatic detailed reporting about your IT infrastructure. It gives you detailed and sustainable reports that validate tests of your IT controls. You can use the built-in Sarbanes-Oxley reports as a part of your IT general control definition and implementation process.

In the section that follows we have developed a template automating IT General Controls for multiple functional areas. In each template we will:

- define a series of internal controls
- defines tests for those internal controls
- identify an Ecora report that documents the test

In some cases there will be no Ecora report because the control is a broad written policy.

Systems Security

Probably the most visible area of IT is security. Many companies have security officers and many audit security of a regular basis.

However, specific to Sarbanes-Oxley, security internal controls aim to provide reasonable assurance that the systems supporting financial reporting are secure against unauthorized use, manipulation, or loss of data. This means both physical and logical controls that support the overall security environment where deficiencies could impact financial reporting.

Systems Security		
Internal Control	Test of Internal Control	Ecora Report for Test
An IT security policy is in place and approved by senior management	Review a copy of the security policy. Evaluate specific areas for compliance.	Not Applicable
	Review security plan to insure relevant financial reporting systems are adequately covered.	Not Applicable
User authentication procedures are followed to insure transaction validity	Ensure strong password and account lockout policies are implemented.	Password Policy
	Ensure appropriate database authentication mode is configured	Authentication Mode
	User session timeout is defined and in place for authorized users	
	Audit and review user privileges on each system	User Privileges
	Audit and review system access permissions to sensitive files	NTFS Permissions
A process exists to review and maintain access rights effectiveness.	Ensure each DBA has own account and no generic accounts used to bypass audit trail of DBA activity	DBA Accounts
	Ensure all logins have passwords and not default password	Login Password
	Review role memberships and permissions to ensure appropriate access and privileges to databases	Role Permissions & Memberships
	Set file system privileges to prevent unauthorized access to database server data files, log files, and backup file	System Privileges

Systems Security continued		
Internal Control	Test of Internal Control	Ecora Report for Test
A process exists to review and maintain access rights effectiveness.	Ensure Verify Function exists and valid to ensure user passwords are validated and strong password criteria required	Verify Function
	Prove adequate password validation in place	Password Lifetime, Password Grace Period, Password Reuse Time, Failed Login Attempts, Password Lock Time
Procedure exists to insure timely action on user account activity: issuing, closing, adjusting	Select sample of terminated employees and determine if their access has been removed	User Access
	Select a sample of new users and determine if access granted matches access approved.	User Access
	Select a sample of current users and review access privileges to determine if rights are appropriate for job function	User Access
	Validate that attempts to gain unauthorized access to financial reporting system are logged and followed up.	Failed Login Frequently Failed Login
A control process exists to review and confirm access rights.	Audit and review user privileges on each system	User Privileges
	Audit and review system access permissions to sensitive files	NTFS Permissions
	Ensure systems configured to restrict anonymous remote access to your systems.	Remote Access
Appropriate controls exist to review and manage remote network access	Audit and review list of linked and remote servers	External Servers
	Identify all public database links. Review and replace with private links as appropriate to restrict access to confidential data	Public Links
	Ensure anti-virus software installed on systems	Computer without Ant-virus Installed

Systems Security continued

Internal Control	Test of Internal Control	Ecora Report for Test
IT Security administration monitors and logs security information and violations reported to management	Determine that a security office or function exists and monitors/reports on security vulnerabilities	Not Applicable
	Review security notable events over past year and management's response.	Not Applicable
Access to facilities is restricted to authorized people and requires identification and authentication	Review written policies and procedures to determine appropriateness.	Not Applicable

Configuration Management

Configuration Management controls ensure that systems are set up and maintained to protect the security, availability, and processing integrity of financial reporting.

Configuration Management		
Internal Control	Test for Internal Control	Ecora Report for Test
Only authorized software is in use on company IT systems.	Review installed applications on all relevant systems.	Installed Application by Computer
System infrastructure is configured to prevent unauthorized access	Confirm that standard server configuration is documented and implemented	Baseline Report
	Review relevant infrastructure components to determine if they adhere to organization's policies.	OS and Service Pack Report by Computer Role
	Ensure all services are configured appropriately and that only required services are running to protect system from unauthorized access	Services Summary
	If using SNMP ensure appropriate Community String(s) defined to prevent unauthorized users from obtaining systems status information	SNMP
Procedures for protection against malicious programs are in place through the use of anti-virus and other software and measures	Ensure systems are updated with appropriate service packs and hotfixes	Patch Levels
	Ensure anti-virus software installed on systems	Computer without Ant-virus Installed
Applications and data storage systems are properly configured to ensure appropriate access control	Evaluate management's frequency of configuration management review	Not Applicable
	Review configuration changes to see if they have been properly approved based on policy.	Consolidated Change Report

Operations

Managing operations addresses how your company maintains reliable systems in support of financial reporting processes.

Operations		
Internal Control	Test for Internal Control	Ecora Report for Test
Management establishes, documents, and maintains standard policies and procedures for IT operations.	Review documented policies and determine if they are reviewed periodically.	N/A
Appropriate audit mechanisms are in place to allow detail event tracking	Ensure strong audit policy configured to ensure audit trail of events is recorded to provide audit trail of user activity (e.g. account login events, policy change, object access, process tracking, etc.)	Audit Policy
	Enable audit events to provide audit trail of user activity	Auditing Enabled
	Enable Archive Log Mode to allow point in time recovery to ensure data not lost when recovering	Archive Log Mode
	Ensure event log settings are configured to retain recorded events for appropriate time and prevent guest access to logs	Event Log
Controls exist to ensure data is collected for tracking user activity	Set Initialization Parameters to provide security and ensure database auditing is active	Initialization Parameters
	Audit and review DB owner for each database	DB Owner

Data Management

Data management controls are used to support information integrity, completeness, and accuracy.

Data management		
Internal Control	Test for Internal Control	Ecora Report for Test
Policies exist for handling, distribution and retention of data and financial reporting output.	Review documented policies and determine if they are adequate and reviewed periodically.	Not Applicable
Retention periods and storage terms for all incoming and outgoing data are clearly defined.	Review written procedures for completeness and adequacy	Not Applicable
A backup and recovery plan has been implemented	Review plan for completeness and relevance.	Not Applicable
	Restore selected configuration data and compare to see if its accurate	Change Report
Confirm no unauthorized changes occur in financial relevant infrastructure	Review selected server configuration data and compare with baseline data	Consolidated Change Report

Summary

Sarbanes-Oxley is a complex and demanding legal requirement. One piece of it is demonstrating IT internal controls. Ecora Auditor Professional can help you quickly and simply demonstrate internal controls with comprehensive reporting and change management processes.

This information presented here is only a preview of the information that Ecora Auditor Professional can deliver to get you started. There are many more configuration settings that impact your server security and many more reports available to provide the in-depth analysis and configuration you require.

Manually collecting this critical configuration information from your servers is time consuming and relies on a human-based process. Companies utilizing a human-based process invest enormous resources and allow tremendous room for human error. A change and configuration management system reduces time and resources and gives you an on-going sustainable process.

Ecora Auditor Professional helps thousands of companies manage their IT infrastructure. A good way is to see for yourself. Therefore, we highly recommend that you use an automated process, configuration management tool: **Ecora Auditor Professional**.

Try Auditor Professional in YOUR environment.

Request a free trial:

<http://www.ecora.com/ecora/register/default.asp>

Ecora has helped over 3,500 companies in 45 countries automate reports for disaster recovery, tracking changes, security, IT audits, and meeting compliance standards. To comply with the Sarbanes-Oxley Act you need to establish internal controls and procedures. Accurate reporting and record keeping are the 'best practices' for IT organizations and business operations.