



## **IT Director's Reference Series**

Practical Guide

To

**Sarbanes-Oxley IT Internal Controls**

## In the **Real** World...

IT managers want easy to install and easy to use management software that fits within their budget and delivers immediate value right out of the box. ...*That's the Ecora promise.*

Ecora provides total configuration management solutions that automate multi-platform configuration reporting, change monitoring, and patch management. Ecora's solutions enhance efficiency and reduce the costs associated with IT compliance, business continuity, and vulnerability assessment while providing the means to monitor change and plan for recovery. Cost effective, easy to implement, and easy to manage IT solutions.

Ecora **Enterprise Auditor** - An indispensable tool for documenting and managing your IT environment. If you're addressing Sarbanes-Oxley, HIPAA, CFR Part 11, or other regulatory compliance acts, Ecora automates and delivers audit-ready reports that improve accuracy and save time and money. Ecora supports enterprise platforms: Cisco Systems, Lotus Domino, Microsoft, Novell, Oracle, HP-UX, IBM, Sun Microsystems, Red Hat, and Citrix.

Ecora **Patch Manager** – Don't let researching and manual patching take over your time – Know You're Patched, Today! Save time and reduce costs with a focused patch management solution featuring an optional-agent technology for the automated deployment of critical patches and unique reporting capabilities for both, IT administrators and managers.

Ecora **Dr. Wi-Fi** - Continuously monitor the availability and performance of mission critical Wi-Fi networks. Dr. Wi-Fi provides IT managers real-time data with easy-to-read "dashboard" reports and proactive alerts.

Ecora **DeviceLock** - Prevent users with USB drives from stealing your data. Halt unauthorized Wi-Fi networks from gaining access to your valuable information and manage user access to devices.

### **Ecora Software – Solutions for Managing IT in the **Real** World.**

For more information about Ecora Software  
[www.ecora.com](http://www.ecora.com) or 1.877.923.2672

# Index

Executive Overview .....	4
Practical Guide to Sarbanes-Oxley IT Internal Controls .....	5
Introduction.....	5
Section 302: Corporate Responsibility for Financial Reports.....	5
Section 404 -- Management Assessment of Internal Controls .....	6
Impact on IT.....	7
What are ‘internal controls?’ .....	7
Controls over IT Systems.....	8
Evaluating IT Relevance.....	8
Internal Control Model .....	9
Scope of Internal Controls .....	10
Testing Internal Controls .....	11
How to Structure IT General Controls .....	12
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.

Sarbanes-Oxley spells this out in 19 lines of the law contained in section 404. 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.

In this document we give a brief overview of the Sarbanes-Oxley law. Our focus is on IT internal controls. We've taken our experience with customers and relevant research to develop some working guidelines for designing, testing, and documenting IT 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 internal control structure.

# ***Practical Guide to Sarbanes-Oxley IT Internal Controls***

## **Introduction**

The Sarbanes-Oxley Act of 2002 was written and enacted in response to some rather large and public failures of corporate governance. Enron, WorldCom, and Tyco became well known brand names for all the wrong reasons. Scenes of C level executives being arrested and “perp-walked” in handcuffs became common TV news fare.

Sarbanes-Oxley 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.

Historically, 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. At the same time this lack of detail has created some confusion as to what constitutes appropriate controls.

Much of the discussion about Sarbanes-Oxley as it relates to IT focuses on two sections: 302 and 404.

## **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 effectively puts IT in the Sarbanes-Oxley compliance game. CEOs and CFOs, who bear full responsibility for Sarbanes-Oxley compliance, quickly find that IT departments are where internal controls at a material level can be implemented, managed, and documented.

## **Section 404 -- Management Assessment of Internal Controls**

When the Sarbanes-Oxley Act was signed into law, it was obvious compliance would require significant effort from financial executives. An area of particular concern was 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.

It also requires an annual assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. Section 404 also requires the company's auditor to attest to, and report on, management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board.

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 all other companies that file periodic reports with the SEC, the compliance deadline is April 15, 2005.

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.

This involves establishing the necessary controls, engaging in risk assessment, implementing control activities, creating effective communication and information flows, and monitoring. When developing this infrastructure the organization must follow a structured internal control framework, such as the Internal Controls – Integrated Framework of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The COSO framework applies to operations, finance, and compliance in the following five areas

1. The control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring

The Public Company Accounting Oversight Board (PCAOB) clearly states in its Auditing Standard No. 2 (March 9, 2004) that,

“Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework

established by a body of experts that followed due-process procedures to develop the framework.....Although different frameworks may not contain exactly the same elements as COSO, they should have elements that encompass all of COSO's general themes.”

Based on PCAOB guidance this document will use the COSO standard in discussing SOX IT controls.

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. There needs to be a good faith effort to attain this compliance by the businesses affected by the act.

The focus of this document is to give an overview of IT compliance as it relates to Sarbanes-Oxley.

## **Impact on IT**

One particularly challenging area of Sarbanes-Oxley 404 involves IT controls, a key area since so many of today's business processes are IT driven. Corporate Sarbanes-Oxley Compliance Teams should include a core team member with an IT background to ensure IT issues are considered during implementation. And a general IT controls section should be included in the documentation of each process and must be completed by a person with an IT background.

Due to the availability of reliable technology, most companies have already regulated themselves to a degree. And have also instituted some form of financial oversight in the form of independent audits.

Since financial data rests on servers, the security and documentation of IT systems is imperative to ensure the integrity of the data placed there. The corporation must have reliable, replicable, and audit proof detail about control of, and access to, the infrastructure that supports financial data.

So what exactly is needed – in an IT sense – to get ready for Sarbanes-Oxley?

Organizations are mandated to implement a series of ‘internal controls’ and procedures to communicate, store, and protect that data. In other words, you need to lock down the IT environment and clearly document how this is done and how it is monitored. Underneath that simple statement lays a wide range of tasks involving a great deal of work. The types and frequency of reports you'll need to create will be dictated by the complexity of your business processes and your company's specific audit and compliance structure/definition.

## **What are ‘internal controls?’**

Defined by COSO, Internal controls are the exercise of best practices. More formally, an internal control is broadly defined as a process, affected by an entity's board of directors,

management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- 1) Effectiveness and efficiency of operations.
- 2) Reliability of financial reporting.
- 3) Compliance with applicable laws and regulations.

## Controls over IT Systems

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.

Control frameworks exist that can facilitate Sarbanes-Oxley compliance efforts. COSO, Committee of Sponsoring Organizations, *Internal Control – Integrated Framework* and CobIT's *Control Objectives for Information and Related Technology* are excellent references for IT controls.

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. Which means that IT management must become intimate with and conversant in 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 Sarbanes 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 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 nonroutine 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?

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

## **Internal Control Model**

A good model to use in looking at internal controls is contained in IT Control Objectives for Sarbanes-Oxley by the IT Governance Institute. Figure 1 is adapted from that document and shows four levels of control.

From an overall view this model helps define the internal control universe needed for IT controls. If you identify the significant accounts in financial statements and the processes and applications you've put some real limitations on your scope of work. It should be noted that from a control perspective all other controls are dependent on IT general controls which reside on the bottom tier of Figure 1.

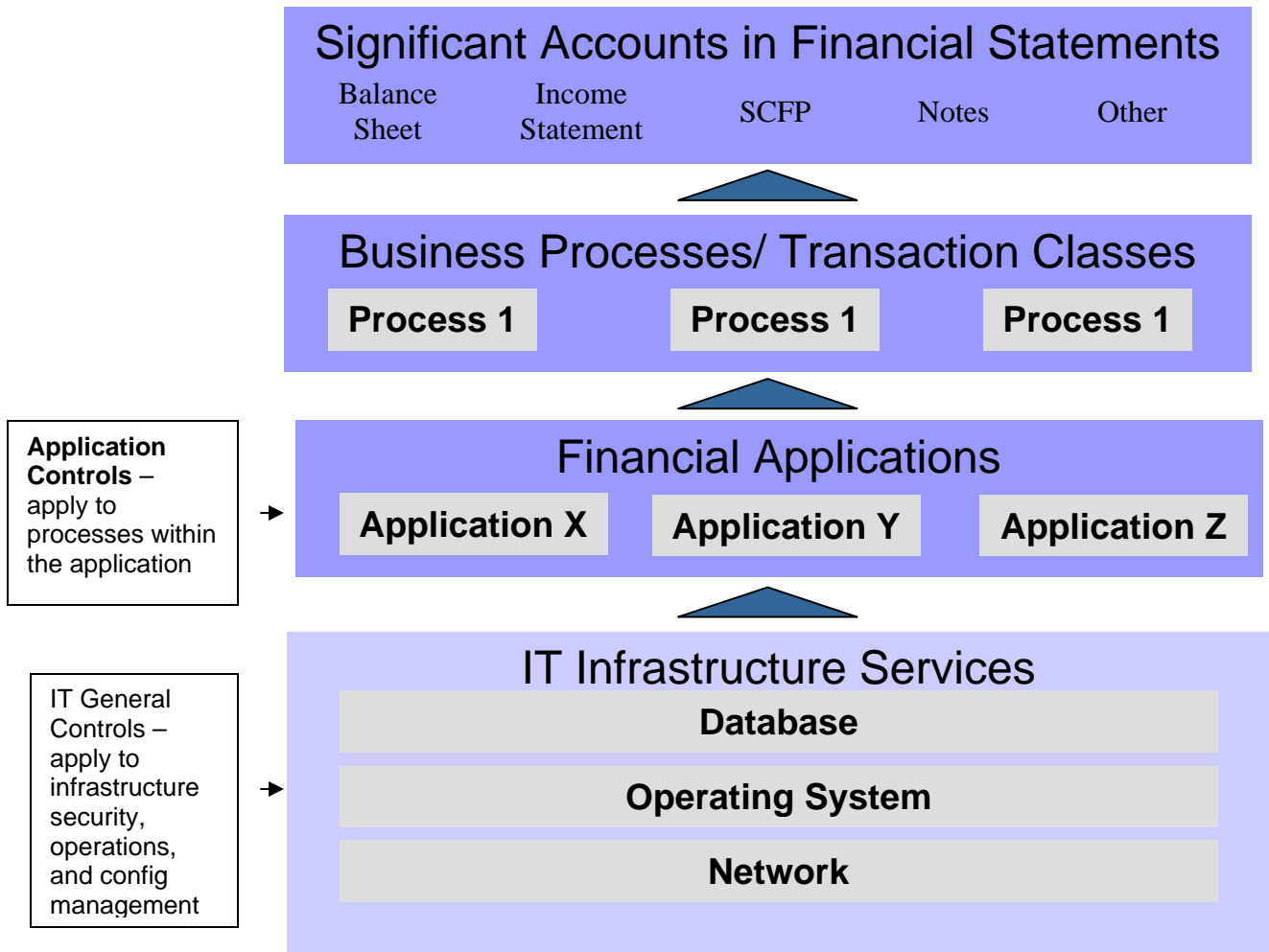


Figure 1. Model for defining IT Controls

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.

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.

**Scope of Internal Controls**

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 2/3 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.

## **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 pat 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.

Today many companies are executing to an internally manageable level in terms of resource, cost, and risk. Then waiting until they experience 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.

### **Ecora Enterprise Auditor and IT Internal Controls**

Ecora Enterprise Auditor 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.

## How to Structure 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.

In the section that follows we have developed a template of 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.

### **Sustainability**

Sarbanes-Oxley is here to stay. Many companies labored long and hard to get ready for their initial audit. Much of that work was by necessity manual. SOX audits are going to be quarterly events and automation is the key to heaving an on-going sustainable system of internal controls.

## 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	<a href="#">User Privileges</a>
	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**

<b>Internal Control</b>	<b>Test of Internal Control</b>	<b>Ecora Report for Test</b>
	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	<a href="#">User Privileges</a>
	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	<a href="#">Computer without Ant-virus Installed</a>

**Systems Security continued**

<b>Internal Control</b>	<b>Test of Internal Control</b>	<b>Ecora Report for Test</b>
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
Procedures for protection against malicious programs are in place through the use of anti-virus and other software and measures	If using SNMP ensure appropriate Community String(s) defined to prevent unauthorized users from obtaining systems status information	SNMP
	Ensure systems are updated with appropriate service packs and hotfixes	Patch Levels
	Ensure anti-virus software installed on systems	<a href="#">Computer without Ant-virus Installed</a>
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 Enterprise Auditor 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 Enterprise Auditor 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. Therefore, we highly recommend that you use an automated process, configuration management tool: **Ecora's Enterprise Auditor**.

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.

**Try Enterprise Auditor in YOUR environment.  
Download a FREE product trial**  
<http://www.ecora.com/ecora/register/default.asp>

Ecora has over 3,000 customers in 45 countries automating reports for disaster recovery, tracking changes, security, IT audits, and meeting compliance standards.

**Ecora Software  
Pease International Tradeport  
2 International Drive, Suite 150  
Portsmouth, NH 03801**

[www.ecora.com](http://www.ecora.com)  
877.923.2672