



The IT Director's Practical Guide
To
Sarbanes-Oxley Compliance

Scott Carpenter, Product Manager
Ecora Software Corporation

Index

Introduction	3
Section 302: Corporate Responsibility for Financial Reports.	3
Section 404 -- Management Assessment of Internal Controls	4
Impact on IT	5
What are 'internal controls?'	6
Controls over IT Systems	6
Evaluating IT Relevance	7
An Approach to Best Practice	7
Report No. 1 -- Domain Admins Group	9
Report No. 2 -- Administrator and Guest accounts renamed	10
Report No. 3 -- Users with Passwords older than 30 days	11
Report No. 4 -- OS and Service Pack Report by Computer Role	12
Report No. 5 -- Share and NTFS Permissions by User	13
Report No. 6 -- Installed Applications by Computer	14
Report No. 7 -- Services Report By Service Name	15
Customer Comments	16
Summary	17

The IT Manager's Guide to Sarbanes-Oxley Compliance

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 framework also includes three categories of controls—effectiveness and efficiency of operations, compliance with laws and regulations and reliability of financial reporting.

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 include a core team member with an IT background to ensure IT issues are considered during implementation. And a general IT controls section is 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?’

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 good frameworks 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?

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

An Approach to Best Practice

'Internal controls' need to be documented and protected from internal, external and unauthorized access, including those that could occur through online systems and networks. Questions that need to be addressed include:

- Who has access to systems holding financial records?
- Who has access to Share information?
- Where are there internal security vulnerabilities?
- What patch levels are we at?
- Are configuration changes being tracked and documented?
- What policies are changing within Active Directory?
- Can we show an audit trail?

A good solution to this problem is to automate the collection of system's data to provide auditors with documented evidence of security best practices.

This is an area where configuration management delivers. You can, for example with Ecora's Enterprise Auditor software, deliver detailed reports about a wide variety of network, servers, and applications that are consistent in content and look and feel, which makes it easy for both you and the auditing entity to understand and explain.

Some standard reports that could be used to validate Sarbanes-Oxley compliant IT infrastructure security model include:

- Domain Structure
- Domain Accounts Policy
- Domain Controller Policy Settings
 - a. Audit Policy Settings
 - b. Event Log Settings
 - c. Security Option Settings
- Group Policy Objects
- Agency-Selected Registry Key Values
- User Accounts Defined in Domain
- Domain Local Groups and Their Members
- Domain Global Groups and Their Members
- Domain Universal Groups and Their Members
- Passwords, 30 Days and Older
- Invalid Login Attempts Greater than "n"
- Accounts With Expired Date
- Disabled Accounts
- Locked Out Accounts
- Rights and Privileges
 - a. Descriptions and General Recommendations for Rights
- Trusted and Trusting Domains
- Servers and Workstations'
- Domain Controllers in the Domain
- Services and Drivers on the Machine
- Logical Drives
- Network Shares

Ecora's Enterprise Auditor provides an elegant solution to documenting your infrastructure and giving you a wide variety of reports that you can tailor to your company's specific Sarbanes-Oxley compliance package. The next section shows some sample reports.

Report No. 1 -- Domain Admins Group

Members of the Domain Admins group have elevated privileges for creating, deleting, and modifying user rights, domain configuration settings, system configuration settings, and much more.

To ensure that only the appropriate personnel have been granted membership to this powerful group, the membership should be regularly reviewed and tracked for changes.

This report not only identifies the membership of the Domain Admin groups but it also reports user account expiration, account lockout, and whether the user is disabled.

Table 1 Domain Admins Group

Domain	User Name	User Full Name	User Account Expires	User Locked Out	User Disabled
DOM	Adow	Adam Dow		No	No
DOM	Administrator			No	No
DOM	bparker	Bill Parker		No	No
DOM	Cmayne	Caitlin Mayne		No	No
DOM	Evirginia	Emily Virginia		No	Yes
DOM	Rsharon	Rosemary Sharon		No	No
DOM	Selizabeth	Sarah Elizabeth	Jan 12 2007 23:00	Yes	No
DOM	Treynolds	Tim Reynolds		No	No
DOM	Vcortez	Victor Cortez	Jan 12 2007 23:00	No	Yes

Report No. 2 -- Administrator and Guest accounts renamed

Best practices dictate that built-in Administrator and Guest accounts should be renamed, as they are a target for people trying to gain unauthorized access to your systems. The guest account should also be disabled.

Best practice also calls for a decoy "administrator" account to be created with no privileges, disabled, and tracked for failed logon attempts. This report identifies whether the built-in Administrator has been renamed and whether Guest accounts have been renamed. If the built-in Guest account has not been renamed, then it reports whether the account is disabled or enabled. If enabled, it states whether the account has Admin or User privileges.

Table 1 Renamed Accounts.

Computer Name	Administrator Account Renamed?	Guest Account Renamed?
CADC001	No	Disabled (not renamed)
CADC002	No	Disabled (not renamed)
CADC003	No	Disabled (not renamed)
CADC004	No	Disabled (not renamed)
CADC005	No	Disabled (not renamed)
CAFP002	Yes	Disabled (not renamed)
CAXC001	No	Disabled (not renamed)
CAXC002	Yes	Yes
FLFP001	No	Disabled (not renamed)
FLFP002	No	Disabled (not renamed)
FLFP003	No	Disabled (not renamed)
FLFP004	No	Disabled (not renamed)
FLFP005	No	Disabled (not renamed)
FLFP006	No	Disabled (not renamed)
FLFP007	No	Enabled as a user (not

Report No. 3 -- Users with Passwords older than 30 days

Security best practices recommend that users change their passwords at regular intervals. Each company's policy on password changes can vary, but a common interval is 30 days. This security report identifies user accounts that have a password older than 30 days.

Table 1 Password Age by Domain.

Domain Name	User Name	User Password Age
Dom	Administrator	291
	ASPNET	48
	Evirginia	40
	Guest	315
	IUSR_ANGEL	54
	IWAM_ANGEL	54
	Jnesper	131
	Revans	291
ChildDom	Administrator	108
	Adow	113
	bparker	108
	Cmayne	113
	Evirginia	108
	Rsharon	113
	Selizabeth	51
	Treynolds	57
NTDom	Administrator	593
	Bgridley	608
	Cmayne	657
	Dmcbride	542
	Fpasters	557

Report No. 4 -- OS and Service Pack Report by Computer Role

This report provides a quick way to make sure all of your computers are at the proper operating system and service pack level. As time grows from when a software vulnerability is identified, so does the likelihood of a mass distributed program that exploits the vulnerability. Outdated operating system and service pack levels increases the risk of such security compromises.

Table 1 Operating System and Service Pack Summary

Computer	OS Name	Service Pack	Computer Role
CADC001	Windows 2000	Service Pack 3	Domain Controller
CADC002	Windows 2000	Service Pack 3	Domain Controller
CADC003	Windows 2000	Gold	Member Server
CADC004	Windows 2003	Gold	Member Server
CADC005	Windows 2000	Service Pack 4	Member Server
CAFP002	Windows 2003	Gold	Member Server
CAXC001	Windows 2003	Gold	Member Server
CAXC002	Windows 2003	Gold	Member Server
FLFP001	Windows 2000	Service Pack 4	Member Server
FLFP002	Windows 2000	Service Pack 4	Member Server
FLFP003	Windows 2000	Service Pack 4	Member Server
FLFP004	Windows 2003	Gold	Member Server
FLFP005	Windows 2003	Gold	Member Server
FLFP006	Windows 2003	Gold	Member Server
FLFP007	Windows NT	Service Pack 6a	Primary Domain Controller
NVWKS0893	Windows 2000	Service Pack 4	Workstation

Report No. 5 -- Share and NTFS Permissions by User

Auditors love to know who has access to which systems and information. This report details Share and NTFS access rights of your network Shares on a user/group basis. This makes it easy to ensure that only appropriate people have been granted **Full Control** to your sensitive information.

Table 1 Share and NTFS permissions by User/Group. Servers

Domain Server	Share Name	Account	Share Permission	NTFS Permission
CADC001	Address	Dom\Domain Users	Allow - Read (RX)	Allow - Change (RXWD)
CADC002	NETLOGON		Allow - Read (RX)	Allow - Full
CADC003	Resources\$		Allow - Read (RX)	Allow - Read (RX)
CADC004	SMSLOGON		Allow - Full	Deny - special (Create Files, Write Data) Deny - special (Create Folders, Append Data) Deny - special (Write Extended Attributes) Deny - special (Delete Subfolders and Files) Deny - special (Write Attributes) Deny - special (Delete)
CADC005	SYSVOL		Allow - Read (RX)	Allow - Full
CADC005	TempAccting	NTDom\Jschmoe	Allow - Full	Allow - Change (RXWD)
CADC005	TempHRInfo	NTDom\Scarlisle	Allow - Full	Allow - Change (RXWD)

Report No. 6 -- Installed Applications by Computer

Auditing systems to identify inappropriate software that is installed can be key to ensuring the security of your systems. Conversely, knowing which systems do not have a particular application installed (e.g. anti-virus software) is also important to ensuring a secure IT infrastructure. This report identifies the installed applications on a per system basis.

Table 1 Installed Applications Summary

Domain Computer	Installed App Name
CADC002	ActivePerl 5.8.0 Build 806
	Adobe Acrobat 4.0
	D-Link AirPlus Access Point Manager
	Microsoft .NET Framework 1.1
	Microsoft Office 2000 SR-1 Premium
	Microsoft SQL Server 2000
	Norton AntiVirus Corporate Edition
	NVIDIA RIVA TNT/TNT2
	WebFldrs
	Windows 2000 Hotfix - KB823182
	Windows 2000 Hotfix - KB823559
	Windows 2000 Hotfix - KB823980
	Windows 2000 Hotfix - KB824105
	Windows 2000 Hotfix - KB824146
	WinVNC 3.3.3
	WinZip
FLXC009	Internet Explorer Q832894
	LiveUpdate
	Microsoft .NET Framework 1.1
	Microsoft Office 2000 SR-1 Premium
	Norton AntiVirus Corporate Edition

Report No. 7 -- Services Report By Service Name

It is important to know the services running on all your systems, as each service can be an open door for unauthorized access to your systems. WWW, FTP, SNMP, and many other services can be a targeted access point on your network. This report identifies on a per service basis the services installed on your systems and how they are configured (i.e. startup account, start method, and status).

Table 1 Services Summary

Service Name	Startup Account	Start Method	Status	Computer
Indexing Service	LocalSystem	Automatic	running	CAB5GDB31
Indexing Service	LocalSystem	Automatic	running	CADC001
SNMP Service	LocalSystem	Automatic	running	CAB5GDB31
SNMP Service	LocalSystem	Automatic	running	CADC001
SNMP Service	LocalSystem	Automatic	running	CADC002
SNMP Service	LocalSystem	Automatic	running	FLXC009
SNMP Trap Service	LocalSystem	Automatic	Running	CAB5GDB31
SNMP Trap Service	LocalSystem	Manual	not running	CADC001
SNMP Trap Service	LocalSystem	Manual	not running	CADC002
SNMP Trap Service	LocalSystem	Manual	not running	FLXC009
Telnet	LocalSystem	Automatic	running	CAB5GDB31
Telnet	LocalSystem	Disabled	not running	CADC001
Telnet	LocalSystem	Disabled	not running	CADC002

Customer Comments

“When we first heard about the IT requirements for Sarbanes-Oxley we thought it would be an unattainable task. With the compliance deadline quickly approaching we needed a solution that worked, *fast*. Ecora’s Enterprise Auditor proved its value immediately with detailed reporting for compliance and the ability to be up and running quickly. Now IT is generating the reports we need, without the manual effort or additional staff.”

– *Scott Robison, Zale Corporation*

“Auditor change reports have saved us a bunch of grief. We run comparisons month-to-month and get a quick look at what’s happening with database metrics, for example. We keep our system ready for growth.”

—*Jim Day, System Administrator, Florida Surplus Lines*

“Ecora Software is giving us audit-ready reports that show detailed configurations of our servers and routers. We just finished a major upgrade of our servers, added additional servers, and replaced our network equipment with Cisco gear. We were in the middle of the project when we were notified that we had to performance an IT audit. We were desperate for a tool that could quickly prepared us for a last-minute GLBA audit, Our documentation of these devices was not complete and what took us only an hour with Ecora would have taken weeks manually.”

- *Karen Sullivan, Director of IT, Publix Employees Federal Credit Union*

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**.

Try Enterprise Auditor in YOUR environment for 2 weeks.

Download a free trial:

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

Ecora has helped over 13,000 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.