



Cressida Technology Ltd
1 Lammas Gate, 84a Meadrow
Godalming, Surrey
GU7 3HT, UK

Tel: +44 01483 239300
Fax: +44 01483 239383
Email: info@cressida.info
Website: www.cressida.info

The Ecora logo consists of the word "ecora" in a bold, blue, lowercase sans-serif font. The letter "e" is lowercase, while "c" is lowercase and "o" is lowercase. The letters "r" and "a" are lowercase. The logo is positioned in the upper right quadrant of the page.

ecora

A vertical photograph of a server rack in a data center, showing multiple server units with blue and white panels. The image is slightly blurred and has a soft, blue-tinted light effect, serving as a background for the left side of the page.

“Must-Have” Security Reports For Sarbanes-Oxley Compliance

**Critical configuration settings
that indicate the security of your servers**

Sample Reports

Sam Carlisle, Product Manger
Ecora Software Corporation

Cressida Technology Ltd. t +44 1483 23 93 00
84A Meadrow f +44 1483 23 93 83
Godalming, Surrey e info@cressida.info
GU7 3HT, UK w www.cressida.info



Index

	Page
Introduction	3
The Sarbanes-Oxley Act and Ecora Best Practices	4
Ecora and Sarbanes-Oxley Matrix	5
Report 1: Domain Admins Group	6
Report 2: Administrator and Guest Accounts Renamed	7
Report 3: Users with Passwords older than 30 Days	8
Report 4: OS and Service Pack Report by Computer Role	9
Report 5: Share and NTFS Permissions by User	10
Report 6: Installed Applications by Computer	11
Report 7: Services Report by Service Name	12
Customer Comments	13
Summary	14

Introduction

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.

Ecora can provide the software solution with information you need for compliance, security, change tracking, and disaster recovery.

It's NOT too late to generate the information you need!

A must have for every IT professional -

The reports contained in this document are only a brief sampling of the automated reports available. Enterprise Auditor also handles configuration management for:

Active Directory	IIS
Cisco	SQL
Citrix	Windows
Linux	Novell Netware
Lotus Domino	Oracle
Microsoft Exchange	UNIX

The Sarbanes-Oxley Act

The Security and Exchange Commission enforces the Sarbanes-Oxley Act (SOX) audit on all public companies. Section 404 of the Sarbanes-Oxley Act mandates that all public organizations demonstrate due diligence in the disclosure of financial information. Organizations are also mandated to implement a series of '**internal controls**' and procedures to communicate, store, and protect that data.

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.

Ecora's Approach to Best Practices

These 'internal controls' need to be **DOCUMENTED** and protected from internal, external and unauthorized access, including those that could occur through online systems and networks. With Enterprise Auditor, you can automate the collection of system's data to provide auditors with documented evidence of security best practices. Enterprise Auditor can help answer the following questions:

- 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?
- And much more...

Ecora & Sarbanes-Oxley Matrix

Features	Ecora Enterprise Auditor Solution
Define Relationships	<ul style="list-style-type: none"> *Manage access control and GPOs *Report on users and access rights *Confirm authorized access
Assess Risks	<ul style="list-style-type: none"> *Alert notification *Out-of-the-box reports to identify risks to the security and integrity of the enterprise *Create custom reports to assess hard-to-find configuration details
Manage	<ul style="list-style-type: none"> *Identify patches needed and provide direct link to pull the patch *Document network settings *Identify configuration changes *Identify authorized and unauthorized access and permission changes *Document OS versions and service pack information *Configuration reporting for domains, machines, users, shares and more
Performance and Capacity	<ul style="list-style-type: none"> *Server/workstation hardware and software configurations analysis *Identify unauthorized software applications *Identify files and accounts not accessed in x days *Disk space analysis *Report key system files for unauthorized changes
Continuous Services	<ul style="list-style-type: none"> *Schedule documentation reports to run at regular intervals *Assess and audit network configuration settings *Systems can be restored on documented network configurations, membership, and other logical and physical information
Monitor the Processes	<ul style="list-style-type: none"> *Reporting using IP Addresses *Assess and audit network configuration settings *Pass/fail analysis of the network based on established or custom technical standards
Assurance	<ul style="list-style-type: none"> *Identify audit configurations and policies within the domain, servers and workstations

Report #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 #2

Administrator and Guest accounts renamed

Best practices dictate that the 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. The 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 the Guest accounts has 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 #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 #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 the 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 #5

Share and NTFS Permissions by User

Auditors love to know who has access to which systems and information. This report will detail the Share and NTFS access rights of your network Shares on a user/group basis. This makes it easy to ensure that only the 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 #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 #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

When reviewing security configuration settings, it's not an event; it is a '**process**' that should be done weekly. Configuration changes are made to servers frequently and any lapse in this process will produce detrimental results.

This information is only a preview of the information that Ecora Enterprise Auditor can deliver to get you started securing your servers. 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.