



**ecorda**

**IT Director's Series**

Achieving Sustainable IT Compliance  
to 21 CFR Part 11

**In today's business climate, IT managers must demonstrate cost-effective, sustainable control of the IT infrastructure to ensure a company's profitability.**

**With system complexity increasing exponentially, manually tracking configurations and changes is no longer an accurate, productive or cost-effective option.**

Easy-to-use and deploy, Ecora Change and Configuration Management solutions have helped over 3,500 companies worldwide do more with less by automating system configuration reporting and remediation across the enterprise. Based on best practice frameworks (ITIL, COSO, COBIT), Ecora solutions deliver operational efficiencies, maximum availability, and a greater level of security.

#### **Ecora's Change and Configuration Management Solution Suite:**

**Ecora Auditor Professional** is a powerful configuration and change reporting solution that collects over a million asset, security, and configuration settings from nearly every operating system, database management system, application, and network device found in an IT infrastructure. The configuration settings are stored in a centralized Configuration Management Database (CMDB) for on-demand, accurate auditing, reporting and change control. Ecora Auditor Professional eliminates the resource-intensive, error-prone manual process of managing enterprise-wide configurations and simplifies ongoing compliance with IT security standards and regulations.

Ecora Auditor Professional includes a web-accessible executive dashboard providing at-a-glance validation of compliance to established IT controls, security policies, and configuration standards. The dashboard evaluates configuration information from the CMDB to generate an easy-to-understand pie graph displaying compliant and non-compliant systems as either green (compliant) or red (non-compliant). This enables IT managers to quickly identify non-compliant systems and direct the appropriate personnel to remediate any non-compliant configurations. Dozens of out-of-the-box report and policy templates are included for Sarbanes Oxley, HIPAA, GLBA, 21 CFR Part 11, VISA PCI, FISMA, and NIST IT requirements. You can also create your own reports and policies or customize existing ones.

#### **The Ecora Auditor Professional family also includes:**

**Ecora Auditor Lite** - A free application that collects and reports on hundreds of configuration settings from nearly every system and device in the IT infrastructure. The audit-ready documentation is generated on demand, and archived reports provide an easily accessible audit trail for effective disaster recovery, IT audits, troubleshooting, and consolidations.

**Ecora Auditor Basic** - An upgrade from Auditor Lite that provides additional functionality by offering dozens of ready-made fact-finding report templates for quick, simplified analysis of critical configuration data such as access rights, NTFS permissions, and password settings.

The Auditor product family supports VMware ESX servers; Microsoft Windows and Exchange servers, SQL Server databases, Active Directory, and workstations; HP-UX, AIX, Solaris, RedHat Linux, and Novell NetWare servers; Oracle databases, Citrix and IIS applications; Lotus Domino servers; and Cisco routers.

**For more information about Ecora solutions:**

[www.ecora.com](http://www.ecora.com) or 1.877.923.2672

# Achieving Sustainable IT Compliance to 21 CFR Part 11

## Table of Contents

<i>TABLE OF CONTENTS</i> .....	3
<i>21 CFR Part 11 – An Overview</i> .....	4
<i>Building Sustainable 21 CFR Part 11 Compliance</i> .....	5
<i>1997 -- Part 11 of Title 21 of the Code of Federal Regulations – Electronic Records; Electronic Signatures</i> .....	6
<i>2003 -- Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application</i> .....	7
<i>Change and Configuration Management: What it is and how it can help you gain control</i> .....	8
<i>CCM Cost/Benefits</i> .....	9
<i>Ecora's CCM Solution and 21 CFR Part 11</i> .....	10
<i>A Structured Approach to Audit-Ready Documentation</i> .....	11
<i>Sample Reports</i> .....	16
Administrative Access Report -- Domain Admins Group.....	16
System Security Report -- Administrator and Guest accounts renamed.....	17
Electronic Signatures -- Users with Passwords older than 30 days.....	18
System Documentation -- OS and Service Pack Report by Computer Role.....	19
Logical Security -- Share and NTFS Permissions by User.....	20
System Documentation -- Installed Applications by Computer.....	21
Systems Documentation -- Services Report by Service Name.....	22
<i>Summary</i> .....	23
<i>Appendix A – Summary of “Guidance for Industry - Computerized Systems Used in Clinical Trials”</i> .....	24
<i>Appendix B – Resources</i> .....	28

# Achieving Sustainable IT Compliance to 21 CFR Part 11

## 21 CFR Part 11 – An Overview

In 1997 the FDA introduced Part 11 of Title 21 Code of Federal Regulations; Electronic Signatures (21 CFR Part 11), which requires in-depth evaluation, documentation, management, and auditing around the computer systems used by FDA-regulated companies.

21 CFR Part 11 has had a significant impact on FDA-regulated companies, largely by triggering widespread confusion on how to achieve and maintain compliance. The FDA's original intent with part 11 was to require that companies adopt policies and procedures for computer systems management to ensure ongoing data integrity. The language of part 11 – combined with a general lack of understanding on how to implement system-wide “best practices” - has left many companies struggling with how to comply.

The FDA has tried to address this issue. Since 1997, a variety of guidances have been issued relative to 21 CFR Part 11. All have been withdrawn except the August 2003 *Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application*.

In September 2004, another draft guidance, *Guidance for Industry, Computerized Systems Used in Clinical Trials*, was issued for comment purposes. It addresses a wide range of specific IT requirements and may be the beginning of a clearer IT compliance picture from FDA. (See Appendix A for an overview.)

Until that occurs, 21 CFR Part 11 and the August 2003 Guidance rather succinctly define the compliance rules.

21 CFR Part 11 is not a specific list of what is required. The August 2003 Guidance<sup>2</sup> indicated FDA would “exercise enforcement discretion” to certain aspects of Part 11. By keeping the definition and interpretation broad, FDA places the onus for designing a compliance model on each company.

By taking this regulatory approach, FDA is tacitly acknowledging that it is unreasonable to give detailed instructions for IT systems and software engineering to companies with years of IT experience and expertise.

This created confusion within the regulated community because it appears that FDA is mandating a level of compliance without clearly defining what compliance means. Over the past eight years companies have struggled with this lack of definition and debated about 21 CFR Part 11 expectations and how best to meet them.

This confusion rests, in part, on a misunderstanding of the compliance requirement by companies in general and IT departments specifically. Many see regulatory compliance as an added burden to an already overworked IT department.

Yet when looked at from a best practices standpoint, the FDA regulations provide direction for achieving and maintaining good systems and software engineering

practice. Embracing a compliance effort -- and developing the tools and processes to achieve it -- can have added benefits throughout an organization.

The challenge for most companies remains -- develop and maintain compliance in an ever changing technical environment with rules that are broadly defined. The real world objective for FDA regulated IT departments is get compliant as soon as possible and institute a sustainable, auditable system.

Companies that use technology to accelerate and automate compliance process development and implementation are generally ahead of those who don't. Choosing the right compliance solutions can save you significant time, resources, and money -- and make your effort sustainable.

One such solution is Ecora Auditor Professional. Auditor Professional automates critical elements of your IT system validation process by collecting thousands of configuration settings into natural language audit-ready reports. It provides you with the documented evidence that your systems are configured the way you say they are.

Auditor Professional, a change and configuration solution, gives you a consistent, reliable, third party view of your IT infrastructure. It provides a vehicle for compliance and a foundation for IT security and overall IT control.

### **Building Sustainable 21 CFR Part 11 Compliance**

Compliance begins by building and implementing a model that demonstrates you:

1. understand the rules
2. have a process that shows how you comply with the rule
3. provide documentation that validates your process.

In this guide, we'll review the appropriate 21 CFR Part 11 documentation. We'll also review basic change and configuration management concepts and how they intersect with Part 11 compliance. Finally, we'll review a matrix that shows the relationship between compliance rules, validating statements, and configuration management reports.

You can use this matrix as a working model for your own compliance effort -- with or without Ecora Auditor Professional. The principles are sound and based on our customers' experience.

## **1997 -- Part 11 of Title 21 of the Code of Federal Regulations – Electronic Records; Electronic Signatures**

In March of 1997 the FDA proposed the "Electronic Records; Electronic Signatures" rules. Five months later, in August, the FDA enacted 21 CFR Part 11.

The law applies to all pharmacological, medical device, biotechnology, food, cosmetics, and health care companies regulated by the Federal Food, Drug, and Cosmetic Act and Public Health Service Act.

21 CFR Part 11 establishes requirements to ensure that electronic records and electronic signatures are trustworthy, reliable and generally equivalent substitutes for paper records and traditional handwritten signatures. Electronic records and electronic signatures may be used to meet record and signature requirements of 21 CFR Parts 210 and 211 when Part 11 requirements are met.

As defined by the FDA, "Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."

The electronic record also includes output from instrumentation (digital signals combined with defined parameters for manipulating signals), software code, etc. These regulations apply to records required by a predicate rule, which is a previously published regulation such as Good Laboratory Practice (GLP), and Current Good Manufacturing Practice (cGMP).

According to the FDA, "Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature."

The rule is designed to ensure accurate and trustworthy information that is traceable across multiple systems, business processes, and entities that fall within FDA regulated areas.

The legislation is intended to take advantage of a wider use of new technologies that will improve both the efficiency of FDA-sensitive business processes and speed of operations.

By establishing tight security and user authentication, enabling electronic audit trails, and enforcing record retention, the life science industry can realize the benefits of electronic records and electronic signatures while maintaining compliance.

Although the rule does not require the use of electronic records or electronic signatures, records and associated signatures submitted to the FDA in electronic form must be compliant with Part 11 requirements. Acceptance of the data by the FDA is therefore "... dependent on its ability to verify the quality and integrity of such data during its onsite inspections and audits." This means that data "... should be attributable, original, accurate, contemporaneous, and legible."

## **2003 -- Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application**

Fast forward to 2003. The FDA issued: "Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application." This guidance was issued to show that FDA was reexamining Part 11 and its application to all FDA regulated products. FDA anticipated that Part 11 would be altered as a result of the re-examination.

While the evaluation was underway, FDA stated that it would exercise "enforcement discretion" as it pertained to certain part 11 requirements. And they removed legacy systems (operational before August 20, 1997) from any immediate enforcement action.

However, FDA also pointed out:

"Note that part 11 remains in effect and that this exercise of enforcement discretion applies only as identified in this guidance."

Three primary elements defined the FDA approach:

1. Part 11 would be interpreted narrowly; fewer records would be considered subject to part 11.
2. For those records that remain subject to part 11, enforcement discretion would be exercised with regard to part 11 requirements for validation, audit trails, record retention, and record copying in the manner described in this guidance and with regard to all part 11 requirements for systems that were operational before the effective date of part 11 (also known as legacy systems).
3. All predicate rule requirements would be enforced, including predicate rule record and recordkeeping requirements.

It is important to note that FDA's exercise of enforcement discretion was limited to specified part 11 requirements. All other provisions of part 11, including certain controls for closed systems in § 11.10., continue to be enforced. The FDA specified its intent to enforce provisions related to the following controls and requirements:

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation
- controls for open systems corresponding to controls for closed systems bulleted above requirements related to electronic signatures

## **Change and Configuration Management: What it is and how it can help you gain control**

Few companies completely understand how to control their infrastructure. Many can't tell you exactly how many servers are active – let alone define each server's configuration. 21 CFR Part 11 has forced companies – and IT departments – to examine and define their infrastructure to prove they are in control. In some cases it also forced the opening of IT to external audits for the first time.

The rationale for systematically managing and controlling changes to IT infrastructures goes far beyond 21 CFR Part 11 compliance. If such a system was in place, compliance would certainly be less painful, but IT departments would also quickly optimize productivity with fewer resources being expended on 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, which are industry-accepted standards for implementing sound system management processes. (See Appendix B for more information.) CCM provides accurate and current information about enterprise-wide systems in order to properly plan, conduct, and validate configuration settings and changes, which reduces security risks and 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 sources make security a moving target. (Gartner says 80 percent of attacks come from inside.) 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 and provide on-demand, accurate information when the FDA comes calling. That's where CCM comes in.

In simplest terms, CCM solutions collect, archive, and report detailed system configuration settings and deploy approved configuration changes. By automating and standardizing these processes, accuracy and reliability increase dramatically. There is also a substantial decrease in human resources needed to collect the data – providing almost instant ROI.

Proactive, ongoing management of your existing IT infrastructure significantly improves processes, ensures data security, and enables you to better answer the questions an FDA inspector might ask. At the core of effective systems management is accurate, up-to-date 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 and produce historical audit trails –essential components for 21 CFR Part 11 compliance
- Standardize configuration settings across all systems

- Detect security vulnerabilities
- Understand network dependencies
- Optimize network and system configurations
- Accelerate problem resolution and troubleshooting
- Manage and preserve system knowledge despite IT staff changes
- Speed up Disaster Recovery – limiting downtime

Even without a driver such as 21 CFR Part 11, CCM's reporting and change control capabilities result in time and cost savings that are 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.

## **CCM Cost/Benefits**

One of the highest costs of information systems is the IT staff. Trying to deal with the tasks associated with the initial and continual need for reports on network server compliance can keep IT staff from completing other high priority projects. Software that automatically creates reports on current IT systems configurations and deploys policy-based changes can be less than 10 percent of the cost of hiring an IT professional to do the same and requires minimal time and attention from your current staff.

- The quality, utility, and consistency of the information collected are critical for disaster recovery, IT audits, IT staff training, and certification or accreditation agencies.
- Downtime is minimized because current, consistent, and accurate documentation is available for reference. IT systems should be available at all times to provide real-time availability of critical business data.
- Due to the increasing demand for a decreasing supply of trained IT professionals, staff turnover can be high. Therefore, an efficient method of knowledge retention and transfer is crucial. The right documentation becomes the basis for training new staff with up-to-date information.

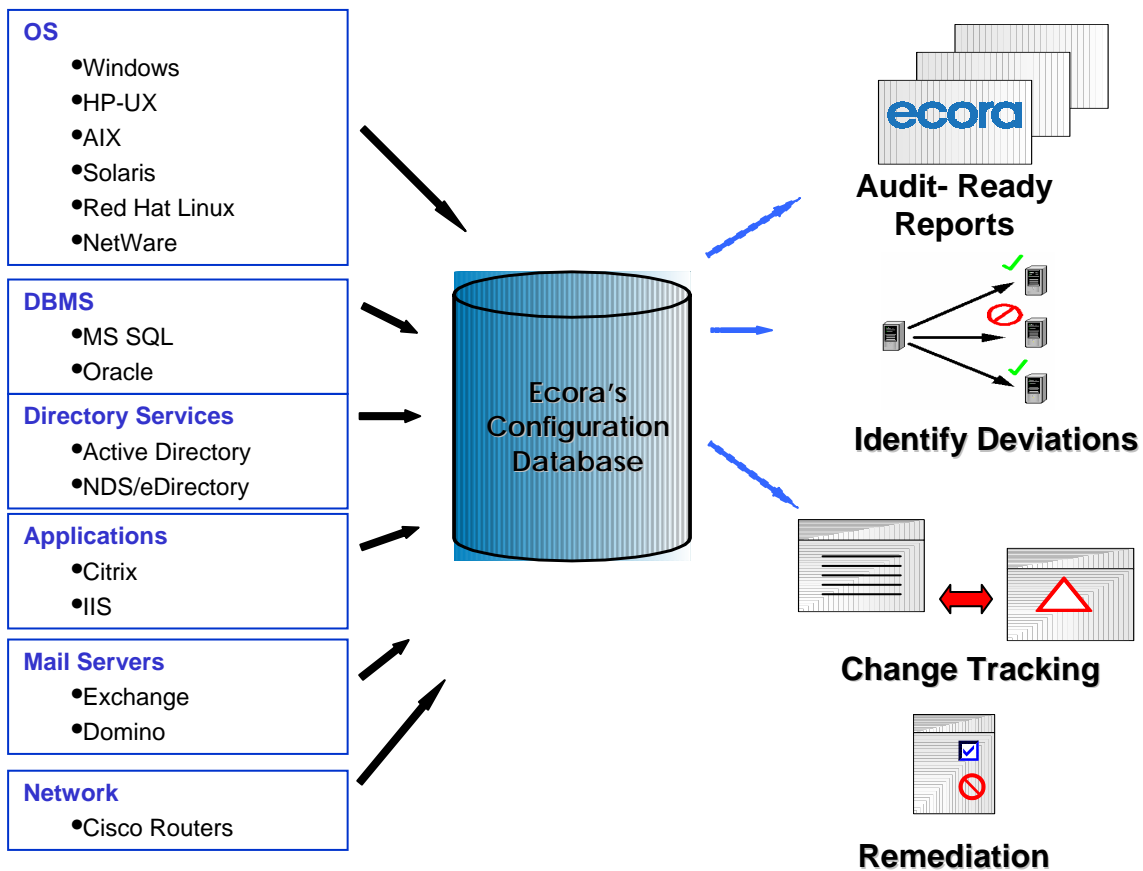
IT management skills and resources are scarce. As more and more organizations move from 21 CFR Part 11 awareness to assessment, development, and implementation sustainable 21 CFR Part 11 compliance plans; demand for these resources will only increase.

## Ecora's CCM Solution and 21 CFR Part 11

The changing landscape of FDA rules keeps one thing constant – you will need to have in place and execute a compliance plan. Ecora can help you achieve that as it relates to your IT infrastructure.

Ecora Auditor Professional automatically collects and reports on thousands of configuration settings. It gives you hundreds of out of the box reports that you can use to prove compliance with access controls, security policies, and configuration standards.

Ecora Auditor Professional collects data from your major infrastructure systems and creates consistent reports, which simplifies the audit process.



**Figure 1.** Ecora Auditor Professional automatically collects hundred of thousands of cross platform configuration settings. It stores that data in a central database and makes it available through hundreds of out of the box and easily customizable reports. It provides a foundation for sustainable IT compliance, security, and control.

## A Structured Approach to Audit-Ready Documentation

Preparing system configuration documentation for IT audits is much like getting ready for an IRS audit. The clearer and more consistent your documentation, the easier it is. Your ability to give an auditor accurate, concise information to questions will speed up the process and in some cases curtail aspects of an audit.

The tables below show how audit documentation can be prepared to help address 21 CFR Part 11 IT infrastructure compliance in a variety of areas. This outline was constructed by referencing the language in the part 11 ruling, as well as the 2003 *“Guidance for Industry Part 11, Electronic Records; Electronic Signatures”* and the 2004 draft of *“Guidance for Industry, Computerized Systems Used in Clinical Trials.”* In the left hand column is a specific guideline contained in the FDA’s Guidance documents. The middle column contains a compliance validation statement. The right-hand column contains a specific existing Ecora Auditor Professional report that proves compliance. Sample reports for some of these rules can be found after the tables.

### DATA ENTRY – Electronic Signatures, Audit Trails, Date/Time Stamps

Electronic Signatures		
Guideline	Compliance Validation	Ecora Report For Validation
Required to ensure that individuals have the authority to proceed with data entry.	Ensure strong password and account lockout policies are implemented.	Password Policy
	Ensure Verify Function exists and is valid, user passwords are validated, and strong password criteria required.	Verify Function
	Ensure event log settings are configured to retain recorded events for appropriate time and prevent guest access to logs.	Event Log
The data entry system should be designed to ensure attributability.	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
Individuals should only work under their own passwords or other access keys and should not share these with others.	Ensure Verify Function exists and is valid, user passwords are validated, and strong password criteria required.	Verify Function

Passwords or other access keys should be changed at established intervals.	Prove that adequate password validation is in place.	Password Lifetime, Password Grace Period, Password Re-use Time, Failed Login Attempts, Password Lock Time
When someone leaves a workstation, the person should log off the system. Or an automatic log off may be appropriate for long idle periods.	Define and implement an automatic logoff period.	Automatic Logoff

<b>Audit Trails</b>		
<b>Guideline</b>	<b>Compliance Validation</b>	<b>Ecora Report For Validation</b>
Maintain an audit trail to protect authenticity, integrity, and, when appropriate, the confidentiality of electronic records.	Ensure a strong audit policy is configured so that an audit trail of events is recorded and an audit trail of user activity provided (e.g. account login events, policy change, object access, process tracking, etc.)	Audit Policy
	Enable Archive Log Mode to allow point in time recovery to ensure data is not lost when recovering.	Archive Log Mode
Secure, computer-generated, time-stamped audit trails must be used to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.	Enable audit events to provide audit trail of user activity.	Auditing Enabled
Audit trails must be retained for a period at least as long as that required for the subject electronic records.	Ensure event log settings are configured to retain recorded events for appropriate time and prevent guest access to logs.	Event Log
People, who create, modify, or delete electronic records should not be able to modify audit trails.	Audit and review user privileges on each system.	User Privileges
	Audit and review system access permissions to sensitive files.	NTFS Permissions
	Ensure systems are configured to restrict anonymous remote access to your systems.	Remote Access
Clinical investigators should retain either the original or a certified copy of audit trails.	Ensure event log settings are configured to retain recorded events for appropriate time.	Event Log
FDA personnel should be able to read audit trails at the study site and at any other location where associated electronic study records are maintained.	Provide detailed audit trail data as requested.	Event Log

Audit trails should be created incrementally, in chronological order, and not allow new audit trail information to overwrite existing data.	Enable audit events to provide audit trail of user activity.	Auditing Enabled
---	--	------------------

<b>Date/Time Stamps</b>		
<b>Guideline</b>	<b>Compliance Validation</b>	<b>Ecora Report For Validation</b>
Controls should be in place to ensure that the system's date and time are correct. Changes to date or time should be documented.	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
	Review selected server configuration data and compare with baseline data	Consolidated Change Report

**System Features**

<b>Change Control</b>		
<b>Guideline</b>	<b>Compliance Validation</b>	<b>Ecora Report For Validation</b>
All changes to the system should be documented	Confirm that standard server configuration is documented and implemented.	Baseline Report
	Review configuration data for changes.	Change Report

## System Security

Logical Security		
Guideline	Compliance Validation	Ecora Report For Validation
Access to the data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.	Ensure that strong password and account lockout policies are implemented.	Password Policy
	Ensure appropriate database authentication mode is configured.	Authentication Mode
	Ensure all logins have passwords and not the default password.	Login Password
	Review role memberships and permissions to ensure appropriate access and privileges to databases.	Role Permissions & Memberships
	Select a sample of new users and determine if access granted matches access approved.	User Access
	Ensure a strong audit policy is configured so that an audit trail of events is recorded and an audit trail of user activity provided (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 should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.	Ensure systems are updated with appropriate service packs and hotfixes.	Patch Levels
	Ensure anti-virus software installed on systems.	Computer without Ant-virus Installed

<b>System Dependability</b>		
<b>Guideline</b>	<b>Compliance Validation</b>	<b>Ecora Report For Validation</b>
Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationships among hardware, software, and physical environment.	Review installed applications on all relevant systems.	Installed Application by Computer
	Review server configurations.	Documentation Report
	Review relevant infrastructure components.	OS and Service Pack Report by Computer Role

**The following section shows you some samples of the preceding reports.**

## Sample Reports

### Administrative Access Report -- 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

## System Security Report -- 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**

<b>Computer Name</b>	<b>Administrator Account Renamed?</b>	<b>Guest Account Renamed?</b>
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

## Electronic Signatures -- Users with Passwords older than 30 days

21 CFR Part 11 explicitly states that passwords should be changed at established intervals. This 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

## System Documentation -- 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**

<b>Computer</b>	<b>OS Name</b>	<b>Service Pack</b>	<b>Computer Role</b>
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

## Logical Security -- Share and NTFS Permissions by User

21 CFR Part 11 mandates that you know and document 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
CADC005	TempHRInfo	NTDom\Scarliste	Allow - Full	Allow - Change (RXWD)

## System Documentation -- Installed Applications by Computer

FDA regulations require you to document the relationship of software and hardware. 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

## Systems Documentation -- 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

## Summary

21 CFR Part 11 is a complex and demanding legal requirement. One piece of it is demonstrating control over your computer systems. Ecora Auditor Professional can help you quickly and simply demonstrate a comprehensive configuration reporting and change management process.

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 information you need to achieve and sustain IT system compliance.

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 configuration management solution: **Ecora's Auditor Professional**.

**Try Auditor Professional in YOUR environment.**

**Download a free trial:**

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

## **Appendix A – Summary of “Guidance for Industry - Computerized Systems Used in Clinical Trials”**

In September of 2004, the FDA reiterated and tightened up the rules around computer systems used in clinical trials. Specifically they refer to:

“computerized systems being used to create, modify, maintain, archive, retrieve, or transmit clinical data. Although the primary focus of this guidance is on computerized systems used at clinical sites to collect data, the principles set forth may also be appropriate for computerized systems at contract research organizations, data management centers, and sponsors. Persons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form.”

The draft Guidance covers a wide range of specific areas starting with general principles, SOPs, and data entry user access. The effect is a quite detailed set of parameters clearly defining a set of documented behaviors around computer systems.

### **General Principles**

Under general principles the FDA cites 9:

1. Identify at which steps a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit data.
2. For each study, documentation should identify what software and hardware is used in computerized systems that create, modify, maintain, archive, retrieve, or transmit data. This documentation should be retained as part of study records.
3. Computerized systems should be designed: (1) So that all requirements assigned to these systems in a study protocol are satisfied (e.g., data are recorded in metric units, requirements that the study be blinded); and, (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.
4. The design of a computerized system should meet the same standard as paper documents in terms regulatory requirements for recordkeeping and record retention.
5. Clinical investigators should retain original or a certified copy of all source documents sent to a sponsor or contract research organization, including query resolution correspondence. Source documents should be retained to enable a reconstruction and evaluation of the trial.
6. When original observations are entered directly into a computerized system, the electronic record is the source document.
7. Changes to data stored on electronic media will always require an audit trail. Documentation should include who made the changes, when, and why they were made.
8. Data should be retrievable so that all information regarding each individual subject in a study is attributable to that subject.
9. Security measures should be in place to prevent unauthorized access to the data and to the computerized system.

## **STANDARD OPERATING PROCEDURES**

FDA reconfirmed the requirement of onsite availability of Standard Operating Procedures (SOPs) relating computerized systems:

SOPs should be established for, but not limited to:

- System Setup/Installation
- Data Collection and Handling
- System Maintenance
- Data Backup, Recovery, and Contingency Plans
- Security
- Change Control

## **DATA ENTRY**

FDA places emphasis on data entry with explicit recommendations about e-signatures, audit trails, and date/time stamps.

### **A. Electronic Signatures**

1. Required to ensure that individuals have the authority to proceed with data entry.
2. The data entry system should also be designed to ensure attributability.
3. Individuals should only work under their own passwords or other access keys and should not share these with others.
4. Passwords or other access keys should be changed at established intervals.
5. When someone leaves a workstation, the person should log off the system. Or an automatic log off may be appropriate for long idle periods

### **B. Audit Trails**

1. People who use electronic record systems are required to maintain an audit trail to protect authenticity, integrity, and confidentiality of electronic records.
2. Secure, computer-generated, time-stamped audit trails must be used to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.
3. Audit trails must be retained for a period at least as long as that required for the subject electronic records.
4. People, who create, modify, or delete electronic records should not be able to modify audit trails.
5. Clinical investigators should retain either the original or a certified copy of audit trails.
6. FDA personnel should be able to read audit trails at the study site and at any other location where associated electronic study records are maintained.
7. Audit trails should be created incrementally, in chronological order, and not allow new audit trail information to overwrite existing data.

### **C. Date/Time Stamps**

Controls should be in place to ensure that the system's date and time are correct. Changes to date or time should be documented.

## VI. SYSTEM FEATURES

FDA focuses system features on tools and processes to help with accuracy and validity of information.

1. **Systems used for direct entry of data** should include features that will facilitate the collection of quality data. Prompts, flags, or other help features should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Electronic patient diaries and e-CRFs should be designed to allow users to make annotations. This information may be valuable in the event of an adverse reaction or unexpected result. The record should clearly indicate who recorded the annotations and when (date and time).
2. **Systems used for direct entry of data** should be designed to include features that will facilitate the inspection and review of data.
3. **Retrieval of Data** -- It is vital that sponsors retain the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the newer systems.
4. **Reconstruction of Study** -- FDA expects to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. Therefore, all versions of application software, operating systems, and software development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained.

## VII. SECURITY

1. **Physical Security** -- In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel. SOPs should be in place for handling and storing the system to prevent unauthorized access.
2. **Logical Security** -- Access to the data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.

Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.

## SYSTEM DEPENDABILITY

The sponsor should ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.

1. Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.
2. FDA may inspect documentation, possessed by a regulated company that demonstrates validation of software.
  1. For software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software.

In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the sponsor or contract research organization should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

2. Documentation important to demonstrate software validation includes:

Written design specification that describes what the software is intended to do and how it is intended to do it;

A written test plan based on the design specification, including both structural and functional analysis; and,

Test results and an evaluation of how these results demonstrate that the design specification has been met.

3. Change Control

Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols.

The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.

All changes to the system should be documented.

## **IX. SYSTEM CONTROLS**

1. Software Version Control

- Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

2. Contingency Plans

- Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.

3. Backup and Recovery of Electronic Records

- Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.
- Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.
- Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

## Appendix B – Resources

For more information on some of the change and configuration management best practice frameworks being implemented worldwide, please visit the following links:

IT Infrastructure Library (ITIL) is a best practices framework for establishing and operating IT service management.

[www.itil.org](http://www.itil.org)

COSO is one of the most widely-accepted internal control frameworks for the audit of internal controls.

[www.coso.com](http://www.coso.com)

Created by the IT Governance Institute, COBIT, Control Objectives for Information and related Technology is an 'open' standard for IT security and control practices.

[www.itgi.org](http://www.itgi.org) or [www.controlit.org](http://www.controlit.org)