



**ecora**

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

Practical Guide

To

Implementing HIPAA IT Security  
Standards



## 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 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.

## **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

## IT Directors Reference Series

### Practical Guide to Implementing HIPAA IT Security Standards

PRACTICAL GUIDE TO IMPLEMENTING HIPAA IT SECURITY STANDARDS .....	4
<i>Introduction</i> .....	4
IT DOCUMENTATION: HOW IT APPLIES TO HIPAA.....	4
<i>What is IT documentation?</i> .....	5
<i>IT Documentation General Benefits</i> .....	5
<i>IT Documentation Cost/Benefits</i> .....	6
<i>The Importance of Server Configuration Settings</i> .....	6
<i>Network and Server Configuration Documentation</i> .....	6
<i>Back-up Tapes and Back-up Documentation for Network Servers</i> .....	7
<i>IT Documentation and Risk Analysis &amp; Risk Management?</i> .....	7
<i>What is the difference between a security audit and an IT audit?</i> .....	8
SPECIFIC HIPAA SECURITY RULES .....	9
<i>Appendix A to Subpart C of Part 164--Security Standards: Matrix</i> .....	9
HIPAA SECURITY STANDARDS.....	11
<i>Administrative, Physical, and Technical Safeguards</i> .....	11
<i>HIPAA IT Security Standards Compliance and Ecora Auditor Professional</i> .....	12
SUMMARY .....	16
SAMPLE REPORTS .....	17
<i>Users with Passwords older than 30 days</i> .....	17
<i>OS and Service Pack Report by Computer Role</i> .....	18
<i>Share and NTFS Permissions by User</i> .....	19
<i>Installed Applications by Computer</i> .....	20
<i>Services Report By Service Name</i> .....	21

## IT Directors Reference Series

# Practical Guide To Implementing HIPAA IT Security Standards

### Introduction

HIPAA, the Health Insurance Portability and Accountability Act of 1996, has probably already had a significant impact on your IT department. The 45 CFR Part 164 security regulations and the April 21, 2005 deadline have broad implications to corporate policies regarding the security and confidentiality of individual health information managed by your IT staff. To ensure compliance and meet federally mandated compliance requirements; organizations must formally evaluate their administrative procedures, networks, and applications to meet HIPAA requirements.

Many health-related businesses have been working to achieve compliance over the past few years. They have parts of the compliance model in place but continue to struggle to build a comprehensive sustainable system. A review of the security standards shows that many of the requirements can be filled with accurate documentation of information held within the configuration data of your infrastructure.

Automation of the IT infrastructure documentation process, with the right tools, can significantly reduce the cost and time of compliance. This paper is about documenting your IT infrastructure as part of a "best business practice" plan for compliance with HIPAA security standards.

### IT Documentation: How it applies to HIPAA

The inevitable evolution of the information age within the health care industry was secured by the passage of HIPAA (Public Law 104-191.) The Final Rule adopting HIPAA standards for the security of electronic health information was published in the Federal Register on February 20, 2003. This final rule (45 CFR Part 164) specifies a series of administrative, technical, and physical security procedures for covered entities to assure the confidentiality of electronic protected health information.

These regulations are far-reaching and require due diligence to compliance on the part of all health care providers, health care plans, and health care clearinghouses, considered "covered entities" under HIPAA. The security regulations set standards for ensuring a secure Information Technology (IT) enterprise-wide network on which the individual identifiable health information is housed.

Compliance can be viewed as an insurmountable task or as an opportunity to develop enterprise-wide solutions to standardize and simplify health information networks. Although this is not a "technology" law, an integral part of compliance to the privacy standards is compliance with the security standards for electronic health information. The protection of private medical information, as covered by the privacy rules, falls under the security rules. The IT architecture within the Information System (IS) plan of an organization is key to the success and compliance of the business.

Building the security strategy of IT networks protects the privacy of individual health information and avoids potential civil and criminal penalties, while reducing the organization's potential security breaches, liability, and possible loss to business reputation. Negative publicity in local and national news compromises a health care organization's standing in the industry and the public's view.

Organizational policies and procedures need to be enterprise-wide to ensure an effective security plan. Individual departmental policies for the secure and confidential handling of private medical information will not meet compliance with HIPAA. Accrediting agencies look for documentation to prove that policies exist and are followed as written. In accreditation terms: "If it isn't documented, it isn't done."

## **What is IT documentation?**

IT documentation is a written record of all the configuration settings on the components of a network. These components include servers, applications, routers, switches, databases, and more. Documentation is needed because these components are extraordinarily complex, configurable, and always changing. Technical staff is often responsible for large numbers of servers and devices, each with a complex collection of settings. IT documentation can provide a central repository of all the relevant information for these settings, their impact, and their values or options.

## **IT Documentation General Benefits**

A thorough understanding of your existing systems significantly improves your planning and management of the IT infrastructure. This process starts with detailed documentation. This has not always been a priority because it requires time and resources. Most organizations rarely (if ever) document IT infrastructures because, until now, 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 "Auditor-Ready" documents on demand
- Detect security vulnerabilities
- Simplify server consolidation and network servers
- Understand dependencies between parts of the network
- Optimize network and system configuration
- Standardize configuration settings across all networks and systems
- Accelerate problem resolution and troubleshooting
- Migrate to new platforms: knowing that baseline and subsequent changes are critical
- Manage and preserve system knowledge despite IT staff changes
- Speed up Disaster Recovery
- Educate new staff and consultants on the organization's IT infrastructure
- Create a standardized "workbook" for outside consultants

Documentation helps streamline migration to new information management applications and new platforms. These products depend on a well-designed network infrastructure. Studying the existing environment prior to migration helps to plan how you want to reconfigure it to make it more efficient.

## IT Documentation 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 documentation of network servers can keep IT staff from completing higher priority projects. Software that automatically documents current network server configurations in minutes in plain-English reports can be less than 10% of the cost of hiring an IT professional to do the same and requires virtually no time / 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 patient health information to those authorized to access it.
- 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.
- Security skills and resources are scarce. As organization's move from HIPAA awareness to assessment, development, and finally implementation of compliance plans; demand for these resources will only increase as the 2005 compliance deadline nears. The sooner core tools are in place, the lower the risk of added expense in a last-minute rush.

## The Importance of Server Configuration Settings

Servers are the last line of IT security defenses. They are managed through their settings. Documenting server configuration settings provides: a record of how the server is configured, a check for inconsistencies and potential security vulnerabilities, and a useful troubleshooting tool. IT system configurations change regularly. Since it is essential that all servers and devices are configured to meet corporate HIPAA compliance plans and policies, IT documentation of server configurations should be a fundamental component of any HIPAA-compliant plan to ensure consistent, documented compliance.

## Network and Server Configuration Documentation

You can document your network and servers manually. However, it is time consuming, seldom current, and often inaccurate. It also uses valuable staff resources for a mundane task. Prior to automation, if network servers were documented at all, it was expensive and tedious. Documenting network servers can also be a record-keeping nightmare. The basic steps, in order of occurrence are:

1. Find all the servers on the network.
2. Find the servers' owners and physical locations (this can take days or weeks depending on the size of the organization).
3. Get access to the servers, assuming the owners are cooperative.
4. Locate, record, and examine configuration settings (this requires knowledge of where settings are stored, access to the data/interfaces, and time to open the applications and files required).
5. Interpret the data and settings gathered. Much or all of the information is in "raw-data" format, requiring definition, organization, and explanation to be comprehensible.

6. Produce a report with varying levels of detail appropriate for various audiences, IT staff, Configuration Auditors, accreditation organizations, and compliance auditors.
7. Return to step 1 and repeat the process continually.

Today, the above steps can be done in less time than it takes to make a cup of coffee. Automated documentation tools are available that build consistent, current, and comprehensive plain-English reports for you. These easily attainable and readable reports of network and server configurations provide valuable knowledge of the IT system. This knowledge is crucial for the optimal use of IT staff and IT budgets.

## **Back-up Tapes and Back-up Documentation for Network Servers**

45 CFR 164 requires all covered entities to have in place contingency plans to recover from emergencies or disasters. It requires:

- Data backup plan
- Disaster Recovery Plan
- Emergency mode operation plan

Backup tapes typically record raw data, not core configuration settings. The tapes are usually stored offline or offsite and the data is retrieved in the event of a problem or corruption. IT system configurations aren't necessarily "backed-up" unless there is a software program on the system specifically designed for this. Most programs only provide server configuration data in partial or raw-data format and the files require a high-level IT professional to decipher and then reconfigure the servers. If you were not the one who originally installed and configured the servers, you might have quite a time restoring the servers without readily available, readable documentation.

Backing up network servers provides information on configuration settings before a disaster occurs. It is important to bring the servers to a state of known configuration settings that worked within the IT security network environment prior to a disaster event. For example, one server might have many different applications that require very specific server configurations on one machine, i.e., Windows NT/2000 and Exchange. Reconfiguring a system from memory or multiple incomplete or generic sources is a fast track to a living nightmare.

## **IT Documentation and Risk Analysis & Risk Management?**

HIPAA security standards require both risk analysis and risk management.

Risk analysis is the process of selecting cost-effective security/control measures by comparing costs of control measures against losses that would be incurred if the measures were not in place. During the analysis, it is important to identify any security risks, assess the probability of an occurrence of a security risk, and analyze the potential adverse impact if a security breach occurs.

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Using IT documentation data can help you discover security vulnerabilities. An on-going automated configuration management system can help manage and mitigate infrastructure risks.

## **What is the difference between a security audit and an IT audit?**

HIPAA defines security as mechanisms to guard data integrity, confidentiality, and availability. The HIPAA Security Matrix is comprised of three categories: administrative, physical, and technical safeguards. Security audits include both physical and informational components of security. Administrative safeguards are information policies such as documenting the IT infrastructure surrounding the data of a healthcare organization: servers, databases, workstations, routers and/or any points of network access.

IT audits encompass some of the physical security audits and all of the information audits. The IT department must have documentation of where hardware components physically exist: the shelf, the room, the floor, the building, the location, the city, and the country. IT audit trail documentation must provide a snapshot of who has access privileges to which servers and if any changes were made to the servers from one point in time to another. They must also document everyone who has physical access to those components at those locations.

The IT department must also audit all of their components from a technology perspective. Configuration settings affect how the components of the network interact with each other from both inside and outside the network. The IT audit provides knowledge that is key to how an organization's network is functioning, to the security of the patient information stored there, and to the survival of the business.

## Specific HIPAA Security rules

The security rules required by HIPAA are spelled out in detail in the *Federal Register, Part II, Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.*

45 CFR 164 Subpart C defines security standards for protection of electronic protected health information. This is where you find specific guidelines and requirements for computer/electronic security. A good summary and reference is contained in Appendix A which is reproduced here.

## Appendix A to Subpart C of Part 164--Security Standards: Matrix

### Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Security Management Process.	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement. (R)

### Physical Safeguards

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Facility Access Controls.	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

### Technical Safeguards (see Sec. 164.312)

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Appendix A segments security standards into Administrative, Physical, and Technical safeguards. IT configuration documentation can provide audit ready compliance within a number of Administrative and Technical areas.

### **Ecora Auditor Professional and HIPAA Security Standards**

Ecora Auditor Professional is configuration and change reporting software. It provides automatic detailed reporting about your IT infrastructure. It gives you detailed and sustainable reports that validate your security standards compliance. You can use the hundreds of built in reports as a part of your Security Standards definition and implementation process.

## **HIPAA Security Standards**

45 CFR 164 requires that covered entities ensure that electronic information is protected in terms of confidentiality, integrity, and availability. This pertains to protected health information created, received, maintained, or transmitted. It also stipulates that compliance is required at the workforce level. It's not enough to have a good plan – you need to make it actionable.

Another requirement is that the security measures you implement must be reviewed and modified as needed to “continue provision of reasonable and appropriate protection of electronic protected health information...” This points out the need to build a system that is self sustaining wherever possible.

The record-keeping burden associated with meeting and maintaining compliance documentation will vary depending upon individual business needs and the size of the organization. The form, format, or degree of documentation necessary to demonstrate compliance is relative to the extent of the IT network.

## **Administrative, Physical, and Technical Safeguards**

The HIPAA security standard is defined in three segments of safeguards: Administrative, Physical, and Technical.

**Administrative safeguards** are policies, procedures, and actions that specify how to define, implement and manage the overall security measures for protected health information. It also include security management of the workforce.

**Physical safeguards** cover physical aspects of a covered entity's electronic information systems protection.

**Technical safeguards** address the technology and the policies and procedures in place to protect the electronic health information it accesses.

IT documentation can play a significant role in preparing covered entities for compliance in the administrative and technical area.

## HIPAA IT Security Standards Compliance and Ecora Auditor Professional

As discussed earlier, IT documentation can help you meet HIPAA compliance mandates. The tables below show how, in the areas of administrative and technical safeguards. This data is meant to be a working template rather than a comprehensive solution.

### A word about sustainability

HIPAA is here to stay. Many companies labored long and hard to get compliant. Much of that work was by necessity manual. HIPAA security requirements – including documentation -- are on-going and automation is the key to having sustainable security compliance.

In the following tables, the first column is a defined security safeguard from 45 CFR164. The second column specifies an action that validates compliance with the safeguard. Column three shows the Ecora Auditor report that documents validation.

Administrative Safeguards		
Security Safeguard	Compliance Validation	Ecora Report For Validation
<p><b>Information system activity review (Required).</b></p> <p>Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.</p>	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 setting are configured to retain recorded events for appropriate time and prevent guest access to logs	Event Log
<p><b>Termination procedures (Addressable).</b></p> <p>Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.</p>	Select sample of terminated employees and determine if their access has been removed	User Access

<p><b>Access authorization (Addressable).</b></p> <p>Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.</p>	<p>Ensure strong password and account lockout policies are implemented.</p>	<p>Password Policy</p>
	<p>Ensure appropriate database authentication mode is configured</p>	<p>Authentication Mode</p>
<p><b>Protection from malicious software (Addressable).</b></p> <p>Procedures for guarding against, detecting, and reporting malicious software.</p>	<p>Ensure systems are updated with appropriate service packs and hotfixes</p>	<p>Patch Levels</p>
	<p>Ensure anti-virus software installed on systems</p>	<p>Computer without Ant-virus Installed</p>
	<p>Review installed applications on all relevant systems.</p>	<p>Installed Application by Computer</p>
<p><b>Log-in monitoring (Addressable).</b></p> <p>Procedures for monitoring log-in attempts and reporting discrepancies.</p>	<p>Validate that attempts to gain unauthorized access to financial reporting system are logged and followed up.</p>	<p>Failed Login, Frequently Failed Login</p>
<p><b>Password management (Addressable).</b></p> <p>Procedures for creating, changing, and safeguarding passwords.</p>	<p>Prove adequate password validation in place</p>	<p>Password Lifetime, Password Grace Period, Password Reuse Time, Failed Login Attempts, Password Lock Time</p>
<p><b>Disaster recovery plan (Required).</b></p> <p>Establish (and implement as needed) procedures to restore any loss of data.</p>	<p>Restore selected configuration data and compare to see if its accurate</p>	<p>Change Report</p>
	<p>Review selected server configuration data and compare with baseline data</p>	<p>Consolidated Change Report</p>

<b>Technical Safeguards</b>		
<b>Security Safeguard</b>	<b>Compliance Validation</b>	<b>Ecora Report For Validation</b>
<p><b>Access control.</b></p> <p>Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).</p>	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
	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
<p><b>Unique user identification (Required).</b></p> <p>Assign a unique name and/or number for identifying and tracking user identity.</p>	Ensure Verify Function exists and valid to ensure user passwords are validated and strong password criteria required	Verify Function
<p><b>Audit controls.</b></p> <p>Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</p>	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 setting are configured to retain recorded events for appropriate time and prevent guest access to logs	Event Log
<p><b>Integrity.</b></p> <p>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction</p>	Audit and review user privileges on each system	User Privileges

	Audit and review system access permissions to sensitive files	NTFS Permissions
	Ensure systems configured to restrict anonymous remote access to your systems.	Remote Access
	Identify all public database links. Review and replace with private links as appropriate to restrict access to confidential data	Public Links
<p><b><i>Mechanism to authenticate electronic protected health information (Addressable).</i></b></p> <p>Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</p>	Set Initialization Parameters to provide security and ensure database auditing is active	Initialization Parameters
	Audit and review DB owner for each database	DB Owner
<p><b><i>Person or entity authentication.</i></b></p> <p>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</p>	Ensure strong password and account lockout policies are implemented.	Password Policy
	Ensure Verify Function exists and valid to ensure user passwords are validated and strong password criteria required	Verify Function
<p><b><i>Transmission Security</i></b></p> <p>Implement technical security measures to guard against unauthorized access to electronic health information that is being transmitted over an electronic communication snetwork</p>	Confirm that standard server configuration is documented and implemented	Baseline Report
	Review relevant infrastructure components to determine if they adhere to organization's policies.	OS and Service Pack Report by Computer Role
	Ensure all services are configured appropriately and that only required services are running to protect system from unauthorized access	Services Summary
	If using SNMP ensure appropriate Community String(s) defined to prevent unauthorized users from obtaining systems status information	SNMP

## Summary

Until recently, creating comprehensive documentation and keeping it current was tedious, time-consuming, expensive, and not legally mandated. Federal HIPAA law makes improved data management and the real-time availability of secure and confidential patient information a critical part of doing business in the health care industry. The common backbone of each of these is the IT systems on which the information resides. The implementation of security matrixes that meet the compliance requirements of HIPAA is best served by having core tools on which to build and maintain an organization's IT infrastructure.

Being able to provide automated documentation of IT servers, with little human intervention, is a technology value-added solution to the HIPAA security compliance requirements facing health care organizations. Best practices need best solutions. Documentation is the key to proving an organization's compliance with HIPAA.

**REMEMBER: IF IT ISN'T DOCUMENTED IT ISN'T DONE**

## Sample Reports

### 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

## 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**

<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

## 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)

## 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

## 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

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

Ecora has over 3,500 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**