



## IT Director's Reference Series

*Configuration Management and Documentation  
to Meet Federal IT Compliance Mandates*

## Index

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| <b>Introduction</b>                                                   | <b>3</b>  |
| <b>The purpose of FISMA:</b>                                          | 3         |
| <b>Key features of FISMA;</b>                                         | 4         |
| <b>NIST Takes Action</b>                                              | <b>5</b>  |
| <b>Configuration Management and Documentation and NIST Guidelines</b> | <b>5</b>  |
| <b>Phase 1 – Initiation</b>                                           | 6         |
| <b>Phase 2- Certification</b>                                         | 7         |
| <b>Phase 3 – Accreditation Phase</b>                                  | 8         |
| <b>Phase 4 – Continuous Monitoring</b>                                | 9         |
| <b>Baselines: Key to Change Management</b>                            | <b>9</b>  |
| <b>Security Template</b>                                              | <b>9</b>  |
| <b>Creating a "Cycle of Control"</b>                                  | <b>10</b> |
| <b>Summary</b>                                                        | <b>11</b> |
| <b>Appendix A – Sample Reports from Ecora</b>                         | <b>12</b> |

## IT Director's Reference Series

### *Configuration Management and Documentation to Meet Federal IT Compliance Mandates*

#### **Introduction**

Managing any aspect of the Federal Government is complex. Perhaps no part of running the country is as complex as the IT infrastructure. Today – just like their counterparts in commercial business – Agencies rely totally on IT.

The IT infrastructure is an agencies most valuable asset, processing the bulk of governmental business transactions, and storing confidential information on all areas of the government, including financial data, human resource records, and email to name a few. Today most of this information is accessible online. And it's all vulnerable. It must be protected constantly and thoroughly without interrupting business.

As an essential – some would say “the” essential -- ingredient for smooth government functioning, IT has been subject to increased regulation and oversight. The elevated security awareness post 9/11 simply adds another level of urgency to tighten up controls and get every agency working to meet higher standards.

In 2002 President Bush signed into law the Electronic Government Act. Title III of the act is the Federal Information Security Management Act or FISMA – see:  
<http://csrc.nist.gov/policies/FISMA-final.pdf>

FISMA made permanent much of the security framework contained in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA requirements are permanent and broader.

FISMA goes beyond GISRA and other legislation on key issues such as accountability and annual testing and evaluation of security controls. It also mandates broader distribution of annual reports.

It requires each federal agency to develop, document, and implement an agency wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source.

#### **The purpose of FISMA:**

1. Provide a framework to insure effectiveness of information security controls of information resources supporting Federal operations

2. Recognize the highly networked nature of the Federal computing environment as a basis for devising effective security management and oversight
3. Provide for development and maintenance of minimum controls to protect Federal information and information systems
4. Provide a mechanism for better oversight of Federal agency information security programs
5. Acknowledge that commercial security products offer a wealth of advanced solutions applicable to security of Federal systems
6. Individual agencies are decision makers when it comes to selecting specific solutions

**Key features of FISMA;**

- The National Institute of Standards and Technology (NIST), collaborating with OMB and agencies, must develop compulsory IT security standards and guidelines for non-classified federal IT systems (classified security systems have their own governance).
- Agencies must develop their own system configuration requirements and provide ongoing monitoring and maintenance.
- Security controls must be tested at least annually.
- Agency CIOs must designate a senior agency information security officer who will ensure FISMA compliance.
- Agencies must provide an inventory of their IT assets.
- 

Given the prominent profile of security concerns and the mammoth size of the federal IT infrastructure, it's not surprising that FISMA is getting increased notoriety and traction.

Congress' findings so far have troubled some in government and politics. In December 2003, a high-profile House subcommittee rated overall federal cyber security a D, up from an F the previous year.

The report card, issued by the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, was doubly significant because for the first time grades were based on FISMA compliance.

## ***NIST Takes Action***

In May of 2004 NIST produced the Guide for the Security Certification and Accreditation for Federal Information Systems. It was developed specifically under FISMA. It provides a clear plan to meet FISMA mandates.

The NIST Guide provides a fairly detailed security and accreditation roadmap with four phases:

1. Initiation
  - a. Preparation
  - b. Notification and resource identification
  - c. System security plan analysis, update, and acceptance
2. Certification
  - a. Security control assessment
  - b. Security certification documentation
3. Accreditation
  - a. Security accreditation decision
  - b. Security accreditation documentation
4. Continuous monitoring
  - a. Configuration management and control
  - b. Security control monitoring
  - c. Status reporting and documentation

With the publication of the NIST guide the onus is now on agency CIO's to build and implement a security process. The window of non-compliance is closing fast.

## ***Configuration Management and Documentation and NIST Guidelines***

NIST guidelines reflect a larger world outside of government. Today all enterprises invest heavily in infrastructure security, often taking a medieval fortress approach: keep the hackers and bad guys out. More often than not, the enemy is within. The Gartner Group forecasts that in the near future 90 percent of all security breaches will originate inside companies.

And even though employees are not stealing secrets, they may be compromising security by flouting IT operating procedures. In one survey, the Gartner Group found that 56 percent of companies had suffered an abuse of computer access controls, and that 78 percent had employees installing or using unauthorized software.

All such activity occurs in what we call the "soft middle," the sections of the enterprise between the firewalls. Particularly vulnerable in this area "inside the perimeter" are servers, switches, routers, and workstations. Common vulnerabilities include:

- Default configurations that are left unchanged
- Default passwords that are left unchanged
- Configuration of unnecessary services
- Latest security patches are not installed

That list focuses on the infrastructure that your whole IT world runs on. Any security plan must include a method for tracking – and documenting that world at a detail level.

In the NIST guideline 4-phase approach a robust configuration management and documentation system is relevant to each phase.

### **Phase 1 – Initiation**

In the initiation phase you need to understand – from a systems perspective -- what you have today. You needed to identify what your infrastructure looks like – and document it at a detailed level. Given the sheer size and scope of federal agencies that, in and of itself, is a monumental task.

Most agencies have some sense of where they are and audits are a way of life. Previous assessments should be a good beginning. However, a sound configuration management system could help deliver an accurate information system description in which the NIST suggests you include:

- Individuals who use and support the information systems, access rights, and privileges
- Hardware and firmware devices
- Systems and applications software
- Hardware, software, and systems interfaces (internal and external)
- Network topology

IT security is traditionally managed with a variety of tools. These include firewalls, intrusion detection systems, vulnerability scanning, and penetration testing. Regardless of the quality of perimeter protection and the frequency of external scans, systems are continually compromised. What part of the security solution is being overlooked?

Time and time again it has been shown that an oversight in operating system or application configuration is a contributing factor in the great majority of system compromises. Products such as Ecora's Enterprise Auditor simplify control through configuration management and assessment. They provide automation in discovery and consistent reporting. Preparation time is reduced and consistency improved, which can result in greater acceptance of the audit process. The process should become routine, a component of regular maintenance.

Traditional system security scanning and analysis tools have a single perspective -- assess only what is apparent from the outside. This leaves internal vulnerabilities of a

complicated infrastructure completely unassessed. Full IT security compliance can only be accomplished with a complete examination of the internals.

There are hundreds of operating system or primary application configuration settings that have implications for security. The manual collection and documentation of the configuration can be a painstaking and time-consuming process -- often a truly Sisyphean effort.

In addition to the size of the task, information can become outdated before the assessment is published. Or worse, a critical configuration changes before a manual assessment is complete. Even the best efforts are prone to error and inconsistency.

Ecora's Enterprise Auditor offers a new perspective from which to view the problem: an inside-out look at network services, interfaces, software feature sets and revisions, and patches and hot-fixes. The resulting documentation includes an evaluation of well-known best practices with tips, notes, and references to additional information. This automation of the process offers a significant advantage in IT assessment, control, and management. It also significantly shortens audit preparation time.

The output you get is a comprehensive collection of configuration data combined with an intelligent assessment and analysis presented in easy to read, plain-English text -- perfect for any auditing process. This output includes the most obscure, yet significant parameters. Workstation-based and agentless, our technology produces immediately useful documentation in browseable HTML and printable formats. A CSV formatted set of configuration parameters is available for export. Visio diagrams of relationship contexts and topologies are provided for overview and holistic analysis.

The feature-rich and accessible documentation is an indispensable security audit deliverable. And it becomes a reference point you can turn to again and again, when you really need to know what's going on inside. Over time, an analyst's knowledge of his infrastructure increases through familiarity of review -- a valuable by-product of the overall assessment effort.

Configuration management includes documentation so that information collected during this phase is consistent, reliable, and usable at checkpoints along the way to certification.

## **Phase 2- Certification**

The certification phase is where documentation is critical. Here NIST says that the information system owner should provide supporting material such as reports, logs, and records showing evidence of security control implementation.

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

Some standard reports that could be used to validate a FISMA compliant IT infrastructure security model include:

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

These reports could easily define an agency's IT Infrastructure security plan. To collect valid information such as this in a dynamic and changing governmental agency is daunting. However, tools exist that make this a rather mundane automatic data collection event.

### **Phase 3 – Accreditation Phase**

The accreditation phase is about distributing the final security accreditation package and updating the plan with the latest information. From a tactical perspective, the work and reports collected in the certification phase constitute a piece of the final report.

## **Phase 4 – Continuous Monitoring**

In the Continuous Monitoring phase NIST addresses configuration management, status reporting and documentation.

Ecora's Enterprise Auditor provides options in scheduling and differential comparisons of configurations. Change Management, in its most elemental form, provides a quick analysis of configuration changes between two documentation sets. This instantly exposes modifications and unintended configuration problems or changes. New environments can be developed to precisely duplicate existing implementations and, conversely, proven environments can be replicated more accurately in the field with documentation and the Change Management function.

### ***Baselines: Key to Change Management***

Baseline documentation sets can be created and implemented as a standardized reference utilizing the Change Management function. Quickly discover which systems do not comply with standardization and which parameters require adjustments. With scheduling options enabled at specific intervals, comprehensive change management can occur. With a quick reference through the Change Management option, systems can be regularly monitored for parameters that deviate from acceptable values.

### ***Security Template***

The first step in implementing Change Management is to develop and use a Security Template. Such a template helps enforce best practices, reduces common vulnerabilities, defines and enforces access rules, and facilitates continuous IT auditing.

A typical security template for a server might include user access and permissions, the disabling of unnecessary defaults, the placement of the latest securities patches, and the monitoring of shared drives. A template for a router would include provisions to address the network's interactive access and the known vulnerabilities of HTTP services.

Resources for creating a Security Template can be found on several Internet sites, including:

CERT (Computer Emergency Response Team) Coordination Center:

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

The SANS (Systems Administration, Networking, and Security) Institute:

[www.sans.org/newlook/resources/](http://www.sans.org/newlook/resources/)

Vendor websites, including Cisco Systems:

[www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl](http://www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl)

The limitation of security templates is they become static documents without the means to incorporate them into some type of automated solution that can regularly monitor an infrastructure. To manually configure, baseline, and monitor every server, router, and

workstation in an enterprise would require armies of people-resources most companies do no have or cannot spare.

When incorporated into Ecora's Enterprise Auditor, security templates serve as the basis for error-proof maintenance of all the configuration settings in an enterprise.

At user-defined points in time, Enterprise Auditor can track over 100,000 changes in an infrastructure: network devices, servers, workstations, databases, and applications. An automated solution can also track configuration changes that impact security, such as access control lists, system user groups, roles and privileges, and router and switch settings.

With general security templates for specific types of IT devices fully developed, and an automated system in place to monitor the infrastructure, the pieces are in place to create a corporate "gold standard" for security and performance-the baseline report.

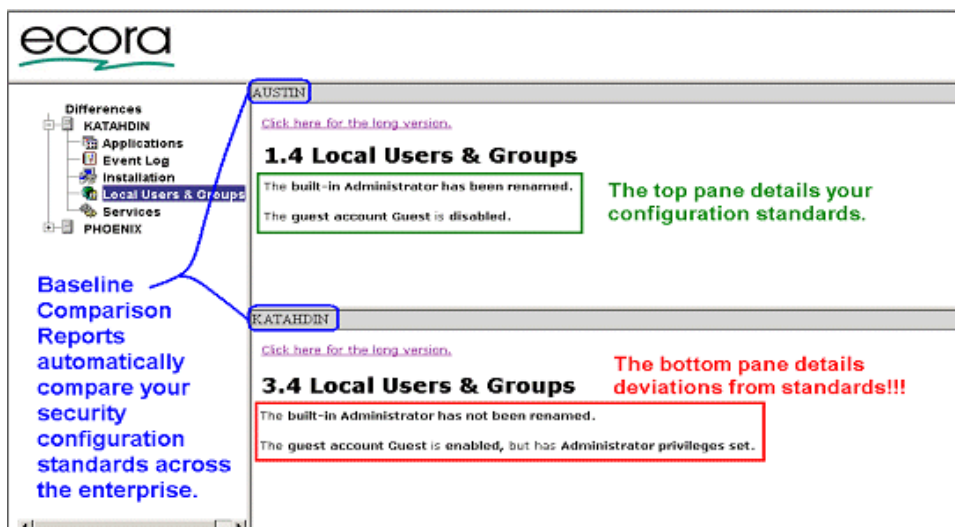
### ***Creating a "Cycle of Control"***

Once security templates are integrated into an automated solution, the final step towards total security lies in creating a "cycle of control," in which performance baselines are established, reports are run to detect instances of noncompliance, settings are reconfigured, if need be, and templates updated-all as part of a regularly scheduled security cycle.

Such a Cycle of Control has three phases:

1. Running Baseline Reports
2. Updating Configurations as needed
3. Verifying changes and updating security templates

Baselining sets and enforces standards. A baseline report is divided into two panes. Reports can be scheduled to run to compare like devices against security templates. The top pane shows a configuration standard. The bottom pane details deviations.



With baseline reports, a routine can be established for doing periodic sweeps of the IT infrastructure to verify that security holes have been plugged, that there is compliance with company policies and best practices, and that security patches have been installed.

This straightforward cycle is an efficient way to harden the soft middle of security, especially in today's environments where networks are in a constant state of change due to mergers and acquisitions, employee turnover, and the endless adding, deleting, and modifying of user accounts and permissions.

Most security breaches occur inside the firewall, in an infrastructure's "soft middle." The best way to tighten up this middle is by developing security templates for each type of network device and using documentation and baseline report features on automated solutions to create a "cycle of control" for all key security settings. This also provides fundamental auditable documentation.

For security audits, automated products such as Ecora provide continuous audits and vigilant tracking of hundreds of security related configuration settings, detailed configuration reports across multiple platforms, and change reports on one IT element or groups of elements.

## **Summary**

FISMA and other federal security mandates are driving increased pressure on agencies to implement and manage a security plan. NIST has added a policy document that clearly stipulates what is required by FISMA.

Good documentation and configuration management can provide the basis for an IT security plan that can meet and exceed the IT infrastructure security requirements of FISMA.

Any security assessment must include inside/out IT management. Controlling what's behind the firewall is just as important and vital as managing external threats. Baselining and configuration change management using tool such as Ecora's Enterprise Auditor provide Security Audit ready documentation that is constantly updated and relevant.

You can quickly and easily implement configuration management controls across the existing network, with baseline comparative documentation a prerequisite "occupancy permit" for the introduction of new systems. Regularly perform enterprise-wide mapping and scanning to ensure compliance with new system introduction and existing controls. Develop a program to reduce the chance that newly deployed applications will introduce unexpected vulnerabilities, and test regularly for unauthorized installations.

## **Appendix A – Sample Reports from Ecora**

This appendix has eight sample reports generated by Ecora Enterprise Auditor. Enterprise Auditor comes with hundreds of out of the box reports that you can use immediately.

Enterprise Auditor can give you configuration settings on much of your critical infrastructure:

|                               |                                    |
|-------------------------------|------------------------------------|
| <b>Applications</b>           | Notes, Exchange, Citrix, IIS       |
| <b>Databases</b>              | Oracle, MSSQL                      |
| <b>OS</b>                     | Windows, UNIX (AIX, Solaris, HPUX) |
| <b>Network Infrastructure</b> | Cisco                              |

In addition it provides detail about what's installed on any given machine – including applications, hardware, and firmware.

To learn more about Ecora Auditor or to get a free trail version simply visit [www.ecora.com](http://www.ecora.com).

**ecora**

## Installed Applications by Computer

**Table 1 Installed Applications Summary**

| Domain Computer       | Installed App Name                              |
|-----------------------|-------------------------------------------------|
| DOMAINA/DENVER        | ActivePerl Build 626                            |
|                       | Adobe Acrobat 4.0                               |
|                       | Aladdin Expander 5.0                            |
|                       | AMS Server                                      |
|                       | Backup2001 Pro V2 Build 106                     |
|                       | Backup2001 Pro V3 Build 104 Version 3 build 104 |
|                       | Belarc Advisor 4.1                              |
|                       | DirectShow                                      |
|                       | DiscJuggler                                     |
|                       | dropcharge ActiveX Control                      |
|                       | Ecora Configuration Solutions for Windows       |
|                       | EcoraSearch                                     |
|                       | Eudora                                          |
|                       | GEAR Pro 5.02                                   |
|                       | HP LaserJet 2100 Software                       |
| iCal 3.5 Web Calendar |                                                 |

Done Internet

**ecora**

## Users with Passwords older than 30 days.

**Table 1 Password Age by Domain or Computer name.**

| Domain Name | User Name            | User Password Age |
|-------------|----------------------|-------------------|
| DOMIANA     | bsplocaluser         | 679               |
|             | test                 | 627               |
| DOMIANB     | Administrator        | 252               |
|             | ASPNET               | 107               |
|             | EcoraReportingCenter | 118               |
|             | IUSR_BOSTON          | 252               |
|             | IWAM_BOSTON          | 252               |
|             | NetShowServices      | 252               |
|             | SQLDebugger          | 105               |

Done Internet



## Services With Non-LocalSystem Service Account

Table 1 Services Summary

| Service Name                  | Startup Account       | Start Method | Status             | Computer             |
|-------------------------------|-----------------------|--------------|--------------------|----------------------|
| ASP.NET State Service         | DOMAINB\IWAM_WIN2K    | Manual       | not running        | DOMAINB/WIN2K        |
| Ecora Patch Manager Service   | .\David               | Automatic    | running            | DOMAINB/W2K3TESTDWL  |
|                               | DOMAINA\barbgallegher | Automatic    | running            | DOMAINA/CODY         |
|                               | DOMAINA\charlierogers | Automatic    | running            | DOMAINA/TCHAIKOVSKY  |
|                               | DOMAINB\administrator | Automatic    | running            | DOMAINB/OMAHA        |
|                               | DOMAINB\administrator | Automatic    | running            | DOMAINB/PORTLAND     |
| DOMAINB\administrator         | Automatic             | running      | DOMAINB/VM-2003CDR |                      |
| Ecora SUS Integration Service | ecora\dennism         | Automatic    | not running        | DOMAINB/VS-SUSSP1    |
| EcoraADRecoveryAgent          | DOMAINB\Administrator | Automatic    | running            | DOMAINB/WIN2K        |
| MSSQL\$CASESENSITIVE          | DOMAINA\barbgallegher | Automatic    | running            | DOMAINA/CHEYENNE     |
| MSSQL\$ECORATEST2000          | DOMAINA\qaservice     | Automatic    | not running        | DOMAINB/TELLURIDE    |
|                               | DOMAINA\qaservice     | Automatic    | running            | DOMAINB/TELLURIDE    |
| MSSQL\$INST2                  | DOMAINA\barbgallegher | Automatic    | running            | DOMAINA/DGLSM2KSQ2K  |
| MSSQL\$MAINE                  | DOMAINB\Administrator | Automatic    | running            | DOMAINB/PORTLAND     |
| MSSQL\$RVIOLA                 | DOMAINB\Administrator | Automatic    | running            | DOMAINB/HEINEKEN2003 |
|                               | DOMAINB\Administrator | Automatic    | running            | DOMAINB/PORTLAND     |

Done

Internet



## Services Report By Service Name

Table 1 Services Summary

| Service Name                            | Startup Account    | Start Method | Status      | Computer          |
|-----------------------------------------|--------------------|--------------|-------------|-------------------|
| Alerter                                 | LocalSystem        | Automatic    | running     | DOMAINA/NEPTSDC   |
| Alerter                                 | LocalSystem        | Automatic    | running     | DOMAINB/BOSTON    |
| Alerter                                 | LocalSystem        | Automatic    | running     | DOMAINB/CROWBAR   |
| Alerter                                 | LocalSystem        | Automatic    | running     | DOMAINB/WIN2K     |
| Alerter                                 | LocalSystem        | Automatic    | running     | DOMAINB/WIN2KDCBU |
| Application Management                  | LocalSystem        | Manual       | not running | DOMAINB/CROWBAR   |
| Application Management                  | LocalSystem        | Manual       | not running | DOMAINB/WIN2K     |
| Application Management                  | LocalSystem        | Manual       | not running | DOMAINB/WIN2KDCBU |
| Application Management                  | LocalSystem        | Manual       | running     | DOMAINB/BOSTON    |
| ASP.NET State Service                   | .\ASPNET           | Manual       | not running | DOMAINB/CROWBAR   |
| ASP.NET State Service                   | DOMAINB\IWAM_WIN2K | Manual       | not running | DOMAINB/WIN2K     |
| Automatic Updates                       | LocalSystem        | Automatic    | running     | DOMAINB/BOSTON    |
| Automatic Updates                       | LocalSystem        | Automatic    | running     | DOMAINB/CROWBAR   |
| Automatic Updates                       | LocalSystem        | Automatic    | running     | DOMAINB/WIN2K     |
| Automatic Updates                       | LocalSystem        | Automatic    | running     | DOMAINB/WIN2KDCBU |
| Background Intelligent Transfer Service | LocalSystem        | Manual       | not running | DOMAINB/BOSTON    |

Done

Internet

**ecora**

## Computers with Yahoo and Kazaa Installed

**Table 1 Workstations**

| Installed App Name            | Workstation Name |
|-------------------------------|------------------|
| KAZAA                         | NEPTSWKS247      |
|                               | NEPTSWKS248      |
|                               | NEPTSWKS262      |
|                               | NEPTSWKS299      |
|                               | NEPTSWKS321      |
|                               | NEPTSWKS366      |
|                               | NEPTSWKS538      |
|                               | NEPTSWKS856      |
| Yahoo! Companion              | NEPTSWKS248      |
| Yahoo! Internet Mail          | NEPTSWKS248      |
| Yahoo! Messenger              | NEPTSWKS248      |
|                               | NEPTSWKS348      |
|                               | NEPTSWKS463      |
|                               | NEPTSWKS674      |
| Yahoo! Messenger Explorer Bar | NEPTSWKS248      |
|                               | NEPTSWKS348      |

Done Internet

**ecora**

## Administrator and Guest accounts renamed.

Best practices dictate that the domain and local Administrator and Guest account should be renamed. The guest account should also be disabled. A decoy "administrator" account can be created with no privileges, disabled and tracked for failed logon attempts.

**Table 1 Renamed Accounts.**

| Domain or Computer Name | Administrator Account Renamed? | Guest Account Renamed? |
|-------------------------|--------------------------------|------------------------|
| DOMAINA                 | Yes                            | Yes                    |
| VM-2003CDR              | No                             | Disabled (not renamed) |
| VM-2K3FRA               | Yes                            | Yes                    |
| VM-2KESNMDAC            | Yes                            | Yes                    |
| VM-2KGER                | No                             | Yes                    |
| VM-2KSERVER             | Yes                            | Disabled (not renamed) |
| VM-AMY                  | No                             | Disabled (not renamed) |
| VM-DEBBIE1              | No                             | Disabled (not renamed) |
| VM-DEBBIE2              | No                             | Disabled (not renamed) |
| VM-ESN2003              | Yes                            | Yes                    |
| VM-FIN                  | Yes                            | Yes                    |
| VM-GERMANXP             | No                             | Yes                    |
| VM-NORVEGIAN            | No                             | Yes                    |
| VS-SMS20                | No                             | Disabled (not renamed) |

Done Internet

**ecora**

## Custom File Report (File Integrity Check)

**Table 1 File Details**

| Device              | Path                                      | NTFS Owner           | Creation Time Day | Creation Time Month | Creation Time Time | Creation Time Year | Size | File Attributes |       |
|---------------------|-------------------------------------------|----------------------|-------------------|---------------------|--------------------|--------------------|------|-----------------|-------|
| DOMAINA/NEPTSWKS395 | c:\Confidential\HR\salaries.mdf           | ECORA\johndoe (user) | 16                | MAR                 | 9:45:31            | 2004               | 486  | Archive         | C369E |
| DOMAINA/NEPTSWKS395 | c:\Confidential\patient data\patients.mdf | ECORA\johndoe (user) | 3                 | MAR                 | 19:11:18           | 2004               | 124  | Archive         | 7A7DF |

Done Internet