

Ten Reasons Why Microsoft Excel Should Not Be Your Documentation Tool

The Perils of Relying on Manual Data Collection
and Documentation

Your IT infrastructure is an integral part of virtually every activity undertaken in your organization on a daily basis. Ensuring the security, performance, and availability of these IT systems is essential to an organization's ongoing success.

In an atmosphere of constant demand for IT services, how do you keep the thousands of infrastructure changes taking place daily from negatively impacting your ability to securely deliver uninterrupted IT services and respond to internal and external audit demands?

Many organizations are still attempting to monitor and control configuration changes manually—using spreadsheets and log books to compile and document data about system changes. If you still find yourself going through this manual exercise, we're going to share 10 reasons that prove you're wasting valuable resources to collect data that simply can't deliver the information you really need.

1 Manual data collection and documentation is inefficient

Even in a small enterprise, attempting to audit and report on configuration changes manually is a time consuming and expensive process. While the cost to document servers manually can vary based on the number of servers in your infrastructure; it represents a significant investment in resources for the average global enterprise. One Midwestern company calculated it was taking 18 hours, on average, to manually document an individual server. With 1530 servers in their environment, they calculated it would take more than 18 full time employees a year to document their servers just once!

Shouldn't these valuable resources be devoted to accomplishing revenue-generating, mission-critical tasks?

"To effectively comply with the new laws and regulations, IT operational groups must be able to document, track, and audit configuration management information. Success will depend on identifying appropriate levels of configuration management item detail, governance, and automation."

—Daniel Vogel
Gartner

Cost to document servers once manually

Server Category	Number of Servers	Time to Document one Server in Hours	Total Number of Days by Server Category
Unix	450	20	1,125
WINNTEL	990	22	2,722
Oracle	39	16	78
Web	20	20	50
MS SQL	31	12	46
Total	1,530	NA	4,021

$$4,021 \text{ days} \div 220 \text{ (working days per person per year) to identify the full time equivalent resource head count} = 18.3 \text{ FTE}$$

- Assumption: \$120,000 fully loaded cost for FTE.
- Cost to document current server configuration once manually = **\$2,196,000**

2 Manual data collection and documentation is error-prone

CRA International was commissioned by Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP, and PricewaterhouseCoopers LLP to review client data from year one Sarbanes-Oxley audits and estimate any changes for the 2006 audits.

The survey concluded that auditors were requiring validation of between 200 and nearly 700 controls in a typical audit. The number of steps required to collect data from a single server alone make the chance of errors during manual data collection and documentation significant. A study on IT-related human error conducted at the University of California at Berkeley revealed the error rate for a simple RAID maintenance task ranged as high as 22.6%. Multiply that by the number of servers in your environment and the likelihood of inaccurate data collection and evaluation grows exponentially.

Plus, if individual departments within your organization are responsible for documenting configuration changes on select groups of servers, differences in scripting or in the way log event files are evaluated can increase the margin for error and inconsistencies in reporting.

RAID System	Total Trials	Trials with Human Errors		Human Error Rate	
		Fatal Errors	Any Errors	Fatal	Overall
Windows	35	1	3	2.9%	8.6%
Solaris	33	0	6	0.0%	17.1%
Linux	31	3	7	9.7%	22.6%

Table 1. Human error rates for simple software RAID maintenance task. On each trial, the human operator was asked to identify and repair a single failed disk in a software RAID volume. Five people participated in the experiments, each carrying out between 5 and 9 trials on each of the three RAID systems. Fatal errors represent situations in which data on the RAID volume was lost, whereas the overall error rate includes trials in which the operator made errors but was able to recover without data loss.

To Err is Human, Aaron B. Brown and David A. Patterson Computer Science Division, University of California at Berkeley

Survey data indicate that the number of key controls tested in year two is expected to decline for both Smaller Companies and Larger Companies.

- *For Smaller Companies, the number of key controls tested by auditors is expected to decline nearly 22 percent on average from 262 to 206 from year one to year two. The average number tested by companies is expected to decline 17 percent from 359 to 298 from year one to year two.*
- *For Larger Companies the average number of key controls tested by the auditor is expected to fall more than 19 percent from 669 in year one to 540 in year two. The average number tested by the company is expected to fall nearly 13 percent from 992 to 867 from year one to year two.*

—Sarbanes-Oxley Section 404 Costs and Implementation Issues: Survey Update, CRA International, December 8, 2005

3 Manual data collection and documentation is not secure

Thousands of changes may take place in your environment at any given point in time, and if they are not controlled, these changes can threaten infrastructure security—today's sophisticated hackers can exploit even the smallest security hole.

This risk is exacerbated when data is collected manually. According to a Benchmark Research Report by the IT Policy Compliance Group released in February 2007, "in one form or another, human error is the overwhelming cause of sensitive data loss, responsible for 75 percent of all occurrences." If you track information like passwords, permissions, and shares manually, and then record them in spreadsheets or log books, you can almost guarantee the information will be exploited.

"User error is directly responsible for one in every two cases [of sensitive data loss]."

—Taking Action of Protect Sensitive Data, IT Policy Compliance Group, February 2007

4 Manual data collection and documentation lacks real visibility

It may sound simplistic, but you don't know what you don't know; most enterprises have only about 10 percent visibility into system changes at any given point in time. It's not unusual to ask an IT manager or administrator how many servers they have and have them answer, "'around 50' or 'between 100 and 110'." If you don't know how many you have, how can you possibly document them? Especially in decentralized environments, it is easy to overlook servers or other hardware.

And, as infrastructures continue to grow in complexity, it is inconceivable that you could track all the changes to these systems manually.

If you can't find them, you can't document them.

"The key to managing perpetual compliance requirements is automated data collection and reporting because it provides visibility into changes across the enterprise in a timely, cost-effective manner."

—Enterprise Management Associates

5 Information is obsolete before a project is complete

With thousands of configuration settings at every level of your infrastructure, it's reasonable to assume your environment is in a constant state of change. Considering that the average server takes 18 hours to fully document manually, it's easy to see just how short a time it takes for manual documentation results to. Especially if you have an extensive infrastructure, your data—or a subset of your data—could potentially be totally obsolete before you've even completed your initial collection.

6 With manual data collection and documentation, there is no way to aggregate data effectively

Often, especially in larger enterprises, the responsibility for collecting and documenting data is delegated among administrators and managed across environments. Ensuring consistency and eliminating errors with this type of process can be a challenge in just a single department. That challenge is heightened considerably when disparate data has to be compiled into a single report. If administrators are using their own scripts to collect data, or, if some are literally logging the information manually, the effort to consolidate data into a single report can be almost as time-consuming and error-prone as the initial collection itself.

7 It is cumbersome to access data that is collected

As challenging as it is to aggregate the data manually, it is even more cumbersome to have to access the data if it was collected manually. The ease of accessing data is particularly critical when specific information is required in preparation for or during an audit or when you're actually troubleshooting a problem. If you are experiencing service degradation or an outage, for example, you will have to scour through massive amounts of data to pinpoint some change that could be the potential root cause for the problem. If you've collected data manually, who knows how long ago the "last known state" was documented and whether it was even accurate? The time required to sort through data manually can result in lengthy mean time to resolution and potential fines if service level agreements are in place.

In the case of an audit, there is no sure way to know what the auditors will ask, and with manual collection, you will have little control over report parameters. It is likely that auditors will require information from a specific date range that is completely different from what you've collected, leaving you to either re-create the report or do a brand-new collection to capture the required data.

According to Gartner, 80 percent of unplanned downtime can be attributed to unstable configuration changes.

8 There is no method for tracking changes

With manual data collection, reports are static, leaving you with no efficient way to merge or compare information to track changes over time. And, even if you have two sets of data to compare, you have no way to be sure that the data has been collected and correlated in the same way both times—especially given the number of configurations in an environment. Visibility into change, as stated earlier, is key to preventing unnecessary downtime. Appropriate change management is also a fundamental requirement of every regulatory compliance mandate.

9 With manual data collection and documentation, there is no institutional memory and no audit trail

When you collect data manually, literally all the documentation you produce is a “one off.” Because an audit trail must be based on similar data collected over time, “one off” reporting cannot produce an accurate audit trail. Studies vary, but, on average, 6-10% of the IT workforce is turning over annually. Given this figure, it is reasonable to expect that historical documentation that was manually collected and prepared was probably done by someone who is no longer with the department or even the company. This causes real deficiencies in reporting, particularly when you are preparing for an audit, because no one may know what methods were used for collection or how the collections were aggregated.

10 Manual data collection and documentation does not scale

When you collect configuration data manually, the process to document each server remains the same, whether you have 100 or 1,000 servers. The process is just going to take a whole lot longer or require a significant number of people (see the table on page XX). In either case, your documentations costs will soar. And, you’ll have to repeat the process more often. Because manual documentation does not scale, you expend more and more valuable resources completing the process or, like many companies, you’ll take your chances and not bother.

“Ecora Auditor Professional makes it easier to find all changes, something we could not have done manually with the amount of servers we’re managing. We’re able to quickly see exactly what changes happened on our servers. If there’s a problem, we’re able to run an historical report, identify the troublesome change(s), and avoid a costly downtime event. Keeping an audit trail also helps us maintain our compliance.”

—Alan Wen
System Analyst
Apache Corporation

Ecora Auditor Professional

Reduce Downtime and Prove Compliance— Automatically

The industry's most comprehensive regulatory compliance and IT best practices reporting solution, Ecora Auditor Professional collects detailed data from across the infrastructure automatically, eliminating the need for manual data collection and documentation.

Once data is collected, Auditor Professional transforms it into easy-to-understand reports that enable you to ensure regulatory compliance and meet IT best practices.

In just days, Auditor Professional delivers value with detailed change and configuration reporting data that enables you to increase system availability, improve uptime, ensure security, and meet compliance audit demands. With Auditor Professional, you will:

- Reduce audit preparation and compliance validation time by 95 percent
- Identify authorized and unauthorized system changes without investing IT staff time
- Shorten the time needed for problem resolution by 80 percent
- Take advantage of identity reporting and access reporting without the time and expense of an identity management system
- Proactively identify system changes and prevent problems
- Deploy disaster recovery reporting, including current system documentation for disaster recovery
- Improve systems availability for greater business value

Find Out More

To find out how Ecora Auditor Professional can help you automate detailed reporting for regulatory compliance audits and enabling IT best practices, call [877.923.2672](tel:877.923.2672) or [+1 603.436.1616](tel:+1603.436.1616), email sales@ecora.com, or visit us on the web at www.ecora.com.

“Ecora helps us do so many things and provides us with such a significant savings that we’ve achieved a return on our investment many times over.”

–Bill Arrington
Network Operating Systems
Boston Children’s Hospital

About Ecora

Ecora Software provides Enterprise Configuration Visibility™ to customers worldwide, ensuring their IT infrastructures are secure, compliant and effective. Ecora is the market-proven leader in transforming enterprise-wide configuration data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's flagship solution, Auditor Professional™, provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for more than 3,600 customers, including many of the Fortune 100. For more information, please visit the Company's Web site at www.ecora.com, or phone [603-334-1616](tel:603-334-1616).

