ecora

WHITEPAPER

Top Ten Keys to Gaining Enterprise Configuration Visibility™

Regulatory compliance. Server virtualization. IT Service Management. Business Service Management. Business Continuity planning. Vulnerability assessments. Information Life-cycle Management. Change Management. Service Level Agreements. IT departments are inundated with a never-ending, diverse list of standards, regulations, initiatives, projects and best practices. As unique as the tasks are related to each of these challenges, they all hold one thing in common. Success depends on being able to produce understandable reports validating expected settings, whether to internal policies or external regulatory standards.

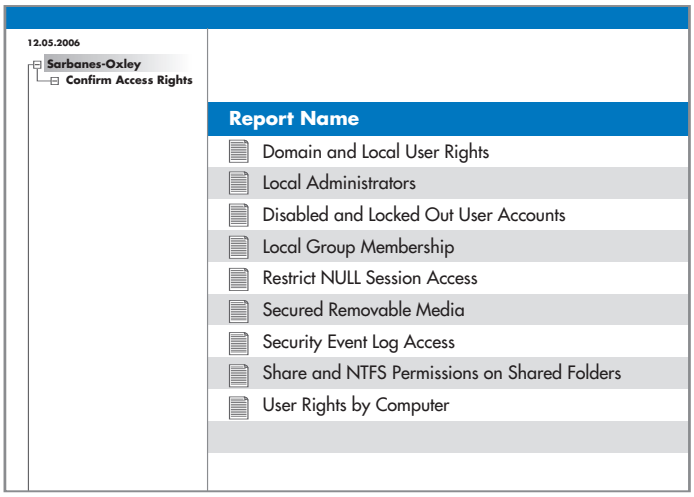
Ecora offers the industry's only solution for automating detailed reporting that ensures Enterprise Configuration Visibility™—reducing the time and cost associated with IT control, compliance, and security, and ensuring the highest levels of availability and performance for your organization.

1 Automate IT Audit and Compliance Reporting and Processes

In this era where new compliance regulations are becoming law on an increasingly frequent basis, organizations are now facing multiple audits from internal auditors and external regulators. With a constant need to prepare for the next audit, critical IT projects can get delayed and hold the business back from implementing important technologies that could provide a competitive advantage.

Ensuring the integrity, confidentiality, and availability of data is the primary objective of these regulations. Each law requires you to prove control over the information in your IT infrastructure and who has access to it. Failure to demonstrate compliance can lead to costly disclosures in a corporation's annual report, substantial financial penalties, jail time, brand-tarnishing press coverage and more.

Manual efforts to collect data and generate reports validating compliance are cumbersome, time-consuming, error-prone, and, ultimately, impractical. **However, with Ecora Software, you can automate IT audit and compliance reporting.** In fact, you can use pre-installed report templates to perform a pre-audit of your IT environment, pinpointing any existing security misconfigurations in your servers. Then, after any problems have been identified and remediated, you can generate up-to-date reports as a deliverable for those auditing your infrastructure.

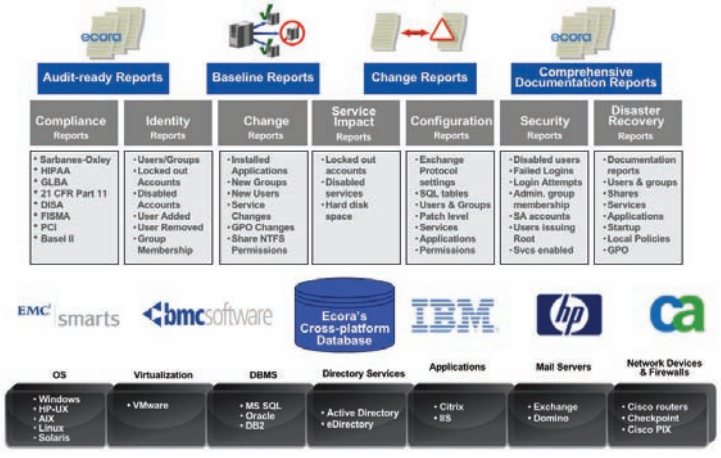


Ecora has worked with thousands of world-wide customers to design out-of-the-box report templates for every major regulatory compliance.

2 Monitor and Identify Any Possible System Change

Controlling the complex relationships among the millions of configuration items in your infrastructure could be the difference between efficiently delivering uninterrupted service to employees and customers or struggling with intermittent service outages, costly slowdowns in transmitting information, and the potential of a security vulnerability being exposed. Maintaining control requires the ability to identify the myriad of changes taking place throughout your environment and quickly pinpointing any potential problems. Even with a change control process in place, it's impossible to validate that approved changes were made correctly—and that there weren't any new, unanticipated changes. Even more critical is the need to find any unauthorized changes that may have been made outside the change control process.

Only Ecora solutions can identify and report on all configuration changes—both approved and otherwise—across virtually any operating system, database, application, and device on your infrastructure.



The value of Ecora's reporting begins with our patented technology for collecting enterprise-wide configuration information. Data can then be integrated into many of today's leading CMDB platforms.

3 Accelerate ITIL Adoption

The ITIL concept emerged in the 1980s, when the British government determined that the level of IT service quality provided to them was not sufficient. Large companies and government agencies in Europe adopted the framework very quickly in the early 1990s. It is now, by far, the most widely adopted IT service management best practice approach in the world. The Information Technology Infrastructure Library (ITIL) is organized into two main areas: service support and service delivery. Service Support includes: Change Management, Release Management, Problem Management, Incident Management, Configuration Management, and Service Desk. Service Delivery involves: IT Financial Management, IT Continuity Management, Capacity Management, Availability Management, and Service Level Management.

The key to rapidly adopting and implementing ITIL standards is an automated reporting solution. **With Ecora solutions, organizations accelerate ITIL adoption through our automated, agentless collection of configuration items vital to all of the Service Support and Delivery disciplines and providing pre-installed report templates to quickly validate appropriate management controls are being maintained.**

ITIL Best Practices	Features	Benefits
Configuration Management	Auditor Professional collects over a million configuration settings from OS, DBMS, Applications and Devices to consistently keep up-to-date information in a CMDB, giving you a very detailed configuration blueprint/baseline of your IT infrastructure.	You always have current and accurate information about your IT infrastructure. Data is available for loading into other CMDB, e.g. BMC Atrium.
Change Management	Automatically identify the actual configuration changes in your environment. Scheduled reporting provides an audit trail of changes overtime. Alerting informs appropriate people of important changes without wasting time reading reports. Remediation provides access-controlled ability to rollback unplanned or undesired changes.	Complement your change management database with the ability to validate agreed-upon changes in your actual IT environment. Find changes that have not gone through the change management process (i.e. unauthorized changes). Use information provided in change reports to expedite change management meetings
Problem Management	We generate change reports for any given time period on any systems. Example: show all changes to all Windows Servers made from January 15th to 16th.	Accelerate problem resolution by knowing precisely what has changed.

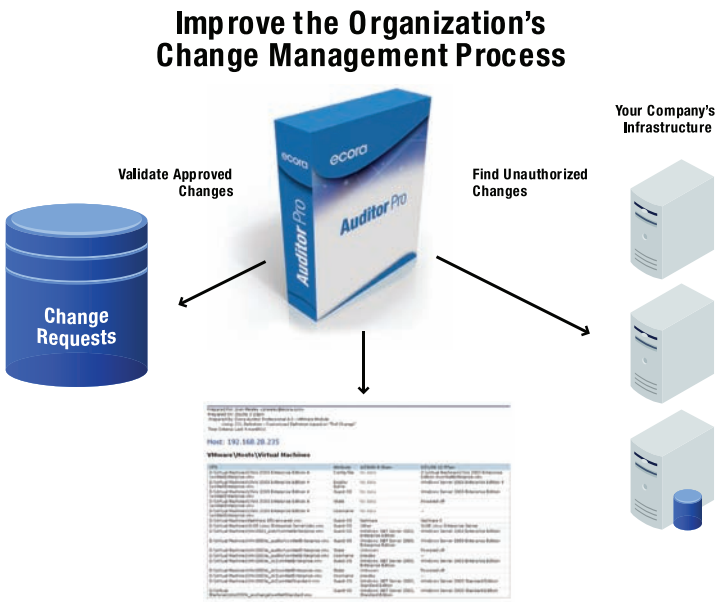
Ecora reports greatly accelerate implementation of ITIL Best Practices.

4 Improve Your Change Management Process By Automating Change Validation

In order to control the negative consequences of uncontrolled change, many organizations have invested in automated solutions for recording changes like BMC Remedy, IBM Tivoli, HP OpenView, or others. While these solutions do bring structure to the change approval process, their weakness is they have no method of identifying whether the approved changes can actually be validated as being deployed in the environment. Even worse, there's no way of identifying changes that have been made outside the official change management process.

Fundamental to any IT best practice standard like ITIL or passing any compliance audit requires the ability to validate approved changes are made and unauthorized changes are identified and remediated—before they cause security problems, degrade performance, or lead to system downtime.

Ecora solutions deliver the data and reports needed to validate authorized changes, identify unauthorized changes or discover any other existing configuration items that deviate from established policies and standards.



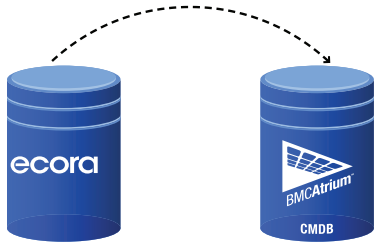
Ecora closes the change management process by validating approved changes are actually completed, while identifying any unauthorized changes.

5 Populate Your CMDB with Data that Matters

In order to effectively manage the complex relationships between the various layers of technology in your IT environment, organizations are looking for processes to centralize control over the information related to the entire infrastructure. For many organizations, especially those adopting IT best practices, the configuration management database (CMDB) serves as the central repository for vital configuration data about operating systems, servers, devices, and more.

Using Ecora's patented technology, organizations can capture more detailed configuration items from operating systems, database management systems, applications, email servers, and network devices than any other solution on the market. For organizations with an existing CMDB, **all of the data collected by Ecora can be federated into an existing CMDB**, such as BMC Atrium. By combining all of the data into a single repository, the insight necessary for initiatives like Business Service Management, Information Life-Cycle Management, and Business Impact Analysis become possible.

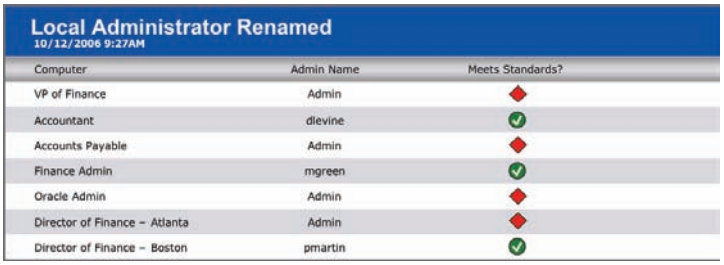
Federate Data Between Ecora's Configuration Database and Leading CMDB's



6 Reduce Audit Preparation Time Through Automation

Regulatory compliance laws governing privileged business and consumer information are growing in number. Today, most organizations are required to be in compliance with several different laws. It's unrealistic for most IT organizations to be well-versed in all of these requirements. Add to that challenge the time required to pull together reports validating each required control. Scripts can be created to gather some of the data, but you still have hours, if not days, to compile it all into a spreadsheet the auditor could understand.

Our team of engineers, working with our global customer base of nearly 4,000 organizations, **has developed hundreds of ready-made report templates** that encompass a complete range of IT best practices and regulatory compliance laws like Sarbanes-Oxley, HIPAA, PCI, GLBA, FISMA and more. Within a few hours of installation, organizations can be generating reports to determine any existing gaps in meeting a given compliance regulation and have clear steps to remediate any problem areas.



Local Administrator Renamed
10/12/2006 9:27AM

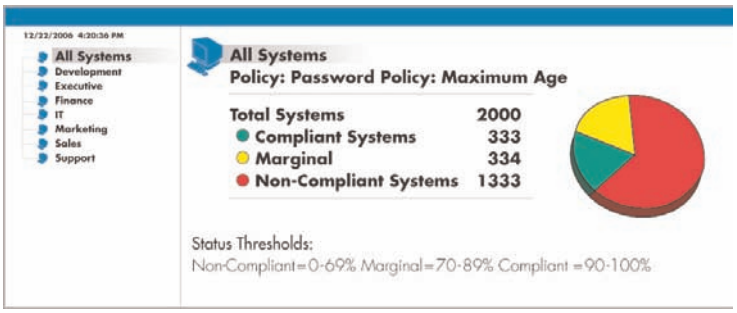
Computer	Admin Name	Meets Standards?
VP of Finance	Admin	◆
Accountant	dlevine	✓
Accounts Payable	Admin	◆
Finance Admin	mgreen	✓
Oracle Admin	Admin	◆
Director of Finance – Atlanta	Admin	◆
Director of Finance – Boston	pmartin	✓

Ecora reports are based on over seven years experience working with our customers to automate their reporting for compliance audits.

7 Automate Validation of Policies and Standards Using Dashboards

Corporate executives have a lot at stake when it comes to regulatory compliance. Years of building brand reputation can be undone by a single security breach. Failing an audit could impact stock values, result in costly penalties, or, worst case, jail time. Yet, no corporate executive has the time to pour through pages of reports to determine whether they're in or out of compliance. Waiting until an audit to determine you're compliant eliminates any opportunity to address any gaps. Today's corporate executive must be able to view enterprise-wide compliance, identify non-compliant systems, and ensure policies and standards are met—at a glance and on demand.

Ecora Auditor Pro's executive dashboard provides an instant analysis of your compliance or non-compliance to internal or external standards using a simple green-red pie chart. The Dashboard evaluates the data collected from the Auditor Pro configuration database by comparing them to pre-built rules based on established information security and regulatory compliance policy standards. The net result is, without the need to generate and analyze reports, you can know what systems are in compliance; what systems are out of compliance; and why they're out of compliance. With Ecora's Executive Dashboard, you quickly and cost-effectively turn compliance into a sustainable activity.

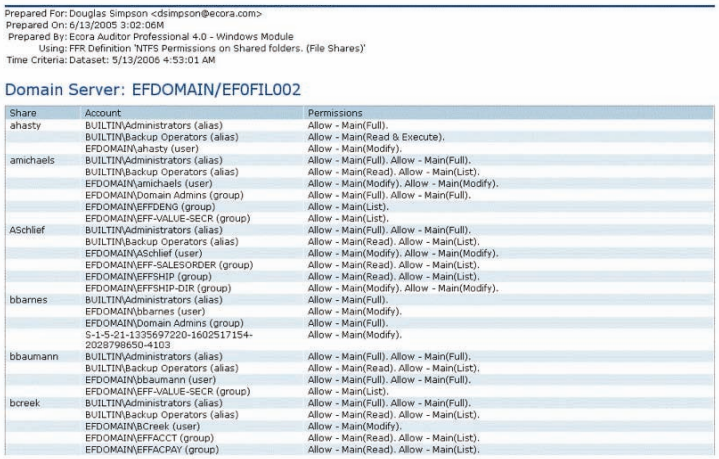


Executive management can monitor enterprise-wide compliance at a glance.

8 Test Your IT Controls

Effective compliance starts with establishing controls to protect privileged information, and then testing those controls continuously to prove you're adhering to them over time. Unfortunately, many companies don't know what controls are needed or how to test them. And the risks are great. If you can't validate your controls continually, you may suffer a security breach, fail an audit, or worse.

With Ecora solutions, you'll benefit from an automated process that will test, validate, and report on IT controls, showing that critical data is protected and satisfying the requirements of any regulatory audit.



Prepared For: Douglas Simpson <dsimpson@ecora.com>
Prepared On: 6/13/2005 3:02:06M
Prepared By: Ecora Auditor Professional 4.0 - Windows Module
Using: FFR Definition 'NTFS Permissions on Shared folders. (File Shares)'
Time Criteria: Dataset: 5/13/2006 4:53:01 AM

Domain Server: EFDOMAIN/EF0FIL002

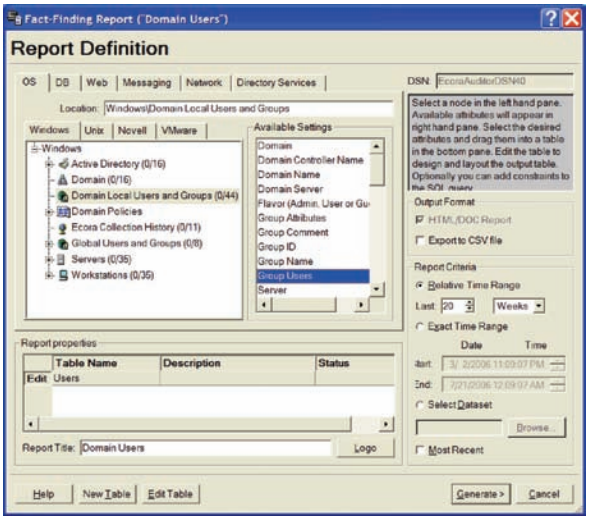
Share	Account	Permissions
ahasty	BUILTIN\Administrators (alias)	Allow - Main(Full).
	BUILTIN\Backup Operators (alias)	Allow - Main(Read & Execute).
	EFDOMAIN\ahasty (user)	Allow - Main(Modify).
amichaels	BUILTIN\Administrators (alias)	Allow - Main(Full). Allow - Main(Full).
	BUILTIN\Backup Operators (alias)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\amichaels (user)	Allow - Main(Modify). Allow - Main(Modify).
	EFDOMAIN\Domain Admins (group)	Allow - Main(Full). Allow - Main(Full).
	EFDOMAIN\EFFDENG (group)	Allow - Main(List).
	EFDOMAIN\EFF-VALUE-SECR (group)	Allow - Main(List).
ASchlief	BUILTIN\Administrators (alias)	Allow - Main(Full). Allow - Main(Full).
	BUILTIN\Backup Operators (alias)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\ASchlief (user)	Allow - Main(Modify). Allow - Main(Modify).
	EFDOMAIN\EFF-SALESORDER (group)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\EFFSHIP (group)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\EFFSHIP-DIR (group)	Allow - Main(Modify). Allow - Main(Modify).
bbarnes	BUILTIN\Administrators (alias)	Allow - Main(Full).
	EFDOMAIN\bbarnes (user)	Allow - Main(Modify).
	EFDOMAIN\Domain Admins (group)	Allow - Main(Full).
	S-1-5-21-1335697220-1602517154-2028798650-4103	Allow - Main(Modify).
bbaumann	BUILTIN\Administrators (alias)	Allow - Main(Full). Allow - Main(Full).
	BUILTIN\Backup Operators (alias)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\bbaumann (user)	Allow - Main(Full). Allow - Main(Full).
	EFDOMAIN\EFF-VALUE-SECR (group)	Allow - Main(List).
bcreek	BUILTIN\Administrators (alias)	Allow - Main(Full). Allow - Main(Full).
	BUILTIN\Backup Operators (alias)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\BCreek (user)	Allow - Main(Modify).
	EFDOMAIN\EFFACCT (group)	Allow - Main(Read). Allow - Main(List).
	EFDOMAIN\EFFACPAY (group)	Allow - Main(Read). Allow - Main(List).

Automated reporting can tell you the "who, what, when, and where" about your data.

9 Know Your IT Infrastructure—Inside and Out

Regulatory compliance and IT Best Practices reporting are not the only challenges IT departments face on a daily basis. An effective reporting solution should provide a wealth of information—about business-critical operating systems, databases, applications, directory services, and networking devices that can be leveraged for solving problems with performance, availability, consolidation, migration, or a myriad of other common tasks assigned to IT.

With Ecora solutions, our patented technology captures more data from across the infrastructure than any other vendor – bar none. Using the hundreds of pre-installed report templates, you can answer virtually any configuration- or change-related question about your IT infrastructure in a fraction of the time it would take using manual processes. Report templates can be customized to answer specific organizational requirements or a report can be quickly created from scratch.



Reports can be easily customized in Auditor Pro's simple drag-and-drop user interface.

10 Identify the Internal Security Misconfigurations Vulnerability Scanners Can't See

Vulnerability scanners, like Digital Eye and Foundstone for example, are valuable for pinpointing security holes in your IT infrastructure that are visible externally, such as open ports. But, industry surveys consistently identify the greatest challenges to your security and vital data are from internal threats. Employees with improper access to systems, files and data and former employees and subcontractors whose access rights haven't been terminated provide some of the greatest threats your organization will face. If you don't control these internal threats, your problems could be compounded by the costs of failing an audit if you're required to comply with regulatory requirements like Sarbanes Oxley, PCI, GLBA, or HIPAA, which all require validation that internal security controls are in place and being followed.

To ensure the complete security of your environment, Ecora solutions offers valuable reports to prevent internal threats, including password aging, user privileges, remote access, consolidated change logs, and more.

Summary

"80% of unplanned downtime is caused by people and process issues, resulting in unstable configuration changes," according to Donna Scott, VP & Research Director for Gartner. Using Auditor Professional, Ecora customers are able to reduce trouble tickets by 22% and, when a trouble ticket is required, they are cleared 50% faster, on average, with Auditor Professional.

Find Out More

To find out how Ecora Auditor Professional can help you ensure IT infrastructures are secure, compliant and effective, call 877.923.2672 or +1 603.436.1616, email sales@ecora.com, or visit us on the web at www.ecora.com.

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.

ecora

2 International Drive, Suite 150 | Portsmouth, NH 03801 | p:877.92.ECORA 603.436.1616 | f:603.436.4344