ecora

WHITEPAPER

Automating Change Management for Security, Compliance, Stability, and Sanity

Alex Bakman
Founder and Chairman
Ecora Software

This whitepaper will review all aspects of change management and present concrete steps you can use to take control of change in your environment.

The Implications of Change

All IT systems are in a constant state of flux, with changes taking place minute by minute. Right now, for example, it is likely that, on your own IT system, someone is installing an application or patch, changing a configuration setting, adding a new user, rolling out a new desktop, or making some other type of change. And even a simple change can greatly impact systems, servers, and applications.

When any change occurs, the infrastructure moves from a "known" state—where systems are secure and operating effectively—to an "unknown" state where it is impossible to be confident that everything is as intended. In fact, any change can have a number of implications, which can impact on everything from operational efficiency, risk management, and business continuity to security, systems integrity, and regulatory compliance.

This occurs because each component and setting in the IT environment is dependent on other components or settings, and every new device or application adds additional settings and new dependencies. This level of complexity makes controlling change more and more challenging.

Let me give you a simple example. An Ecora Software customer had a problem with their Exchange server, so their email wasn't operating. They tried one thing after another to get the server up and running without any success. In the end, the administrator re-installed everything so that the Exchange server—and email—was working again. Everybody was happy, until a security breach was identified several weeks later. You see, when the administrator did the install, he forgot about re-installing the service packs, which had patched some major security problems.

According to Gartner, eight of every ten incidents of unscheduled downtime can be traced to change, and in this case, as in so many others, the problem can be traced to a change.

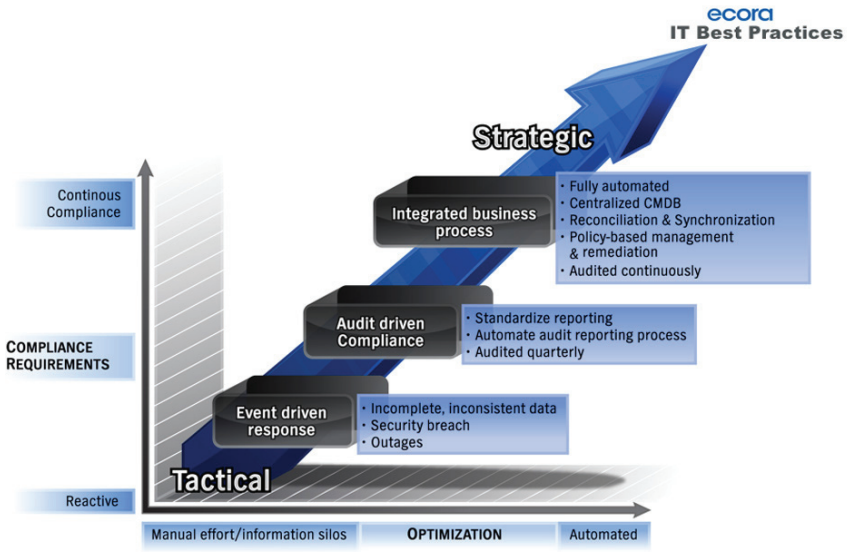
The Evolution of IT Compliance and Best Practices

Almost every organization deals with regulatory compliance requirements on some level, and it is no longer acceptable to be compliant just for an audit alone.

With requirements increasing, expectations for continuous compliance are growing. Financial institutions, for example, may be audited several times each quarter by different regulatory agencies, which necessitates a state of constant readiness—and makes it essential that IT staff members are not tied up in "fire drill mode." These organizations have made compliance a standard procedure so there is no need to "get ready" for an audit. Best business practices are being integrated into daily IT service delivery, controls are in place, and solid reports are available so that these organizations are always ready for an audit.

Change management is at the heart of every regulatory standard. If an organization is not controlling what's changing in the IT infrastructure, the risk of security exposure is great. Unfortunately, many organizations don't consider the relationship between change management and security, and, particularly, the threat that can come from uncontrolled changes made by employees within the organization itself.

How can this type of security issue be discovered and controlled? There are literally thousands of configuration settings—including access control lists, credentials, permissions, password aging, patches, etc.—that control security. All applications have access controls, for example, and if an organization is not monitoring changes to access controls, it can't be completely secure. Similarly, if an organization doesn't control credentials, there is no way to know which unauthorized personnel (or former personnel) may still have access to critical systems. Best practices in configuration and change management lead to a more secure enterprise computing environment.



Regardless of how change management processes are created or which tools are deployed for change management, an organization must control the "what" or "what's changing," the "how" or "how will it be done," the "who" or "who is making the change" for any changes to content, settings, and applications. This is particularly true for those organizations where compliance is a concern.

Preparing for—and Implementing—Change Management

In spite of the obvious importance of change management, 54 percent of respondents to a *Network World* survey reported that they use multiple systems to track all IT operations and application development changes. Fifty-two percent also said that they did not provide any type of change reporting to IT senior management.

So why is the implementation of change management processes so difficult to maintain? According to Gartner, enterprises fail to implement operational change management because they lack governance. If management doesn't pay enough attention or support efforts to control change, an organization can't implement effective change control.

Gartner also says that operational change control requires that IT management adopt change policy guidelines, require process documentation, and automate control and verification processes, and all these elements are critical when preparing for change management.

Preparing for change management begins with a baseline of the IT environment, including effective network and infrastructure documentation from the very beginning of the process. Accurate data can translate into information to guide planning.

Organizations should also create a framework for tracking changes across applications, vendors, departments, project teams, and other stakeholders, and provide a long-term strategy for managing change.

For many organizations, the need to implement a change management process is driven by new regulatory compliance requirements. In these cases, the change management process is often driven from the top. In October 2006, an article in the *Wall Street Journal* said that VISA was targeting the largest 328 retailers to ensure compliance with Payment Card Industry Data Security Standards. Some of these retailers were being fined as much as $100,000 a day for noncompliance. That is a powerful motivation to implementing a change management process to ensure compliance.

Automating Change Management

Change management begins with a focus on processes and on developing a staff that can work with established policies. Automating change management takes processes and policies to the next level and requires advanced technologies including a change management database, change audit and reporting software, a log consolidator, and a CMDB (configuration management database).

Configuration management is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Change management begins with configuration management, and data collected by configuration management tools provides a blueprint for change management processes. In fact, without configuration management, an organization can't have change management, problem management, event management, IT service management, disaster recovery management, IT security, or regulatory compliance.

To automate change management, an organization must:

- Provide a place to record proposed and approved changes
- Enable a workflow-based approval status
- Implement granular, role-based access
- Deploy efficient reporting to ensure consistent measurement
- Implement closed-loop change validation
- Enable detection of unauthorized changes
- Ensure tight integration with the CMDB
- Ensure tight integration with change audit and reporting software

Change Management Goals

- Establish day-to-day business procedures
- Establish and enforce required checkpoints, approvals, and workflow mandates
- Capture, manage, and communicate issues to all team member

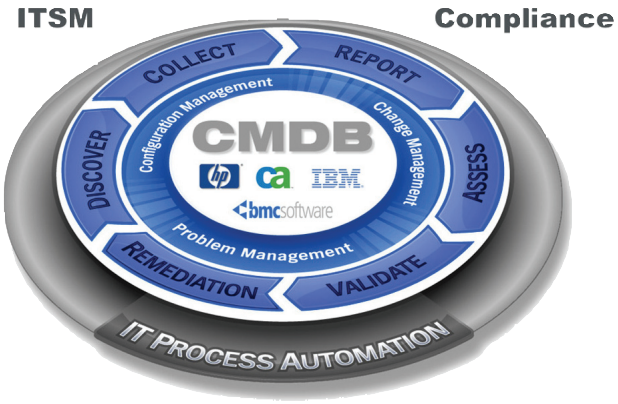
Requirements for Effective Change Management

- Effective communication processes
- Authorization and approval processes
- Comprehensive documentation of all processes and procedures
- Security
- Emergency procedures
- Segregation of duties
- Support from the top

Best Practice Change Management with Ecora Software

Ecora Software delivers out-of-the-box reporting functionality that enables organizations to resolve IT service management and compliance issues efficiently and effectively. With Ecora technology, organizations can leverage the capabilities of the CMDB, extending their investments.

- Auto-Discover to identify systems throughout the enterprise for an accurate inventory. By using a variety of different approaches, auto-discovery prevents rogue systems from going undetected.
- Collect comprehensive data from more operating systems, databases, applications, and network devices than any other configuration reporting software. In fact, Ecora covers more than 80 percent of a typical IT environment, providing a broad view to enable accurate reporting. You'll have the data needed to respond to any configuration or change-related question.
- Report using hundreds of audit-ready report templates. Flexible and customizable reporting functionality allows you to create the specific reports you need, and generate them on a scheduled basis to reduce staff workload.
- Assess the level of compliance using pre-defined policies and rules for compliance regulations and leading information security standards.
- Validate the change management processes and configuration and security policies being followed.
- Remediate problems and automate changes to key security-related configuration settings.



The Results of Sound Configuration and Change Management

Successful configuration and change management begins with clearly defined processes and policies, and a staff willing to work within the requirements. Tools and technologies can certainly be an asset, but even the most powerful tools will be ineffective if processes and policies aren't in place.

If you implement processes and policies for sound configuration and change management, you will realize improved quality of service, reduced downtime, satisfied customers, and a more profitable organization.

To learn how Ecora can help implement successful change and configuration management, call 877.923.2672, email sales@ecora.com, or visit us on the web at www.ecora.com.

What to Look for in Change and Audit Reporting Software

- Broad platform coverage (from hubs and switches to application stacks and everything in between)
- Depth of configuration detail
- Granularity of data selection
- Excellent reporting
- Integration with leading CMDBs and change management databases

About Ecora

Ecora Software is the market-proven leader in transforming enterprise-wide data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's 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 thousands of customers worldwide, 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