

Reining in the Effects of Uncontrolled Change

The value of IT service management in addressing security, compliance, and operational effectiveness

In IT management, as in business as a whole, change is a constant, and can range from the planned, such as application and operating system upgrades, patch installations, and approved configuration updates, to the unplanned, including accidental system alterations and malicious security breaches. Not surprisingly, these “unplanned” changes can have the greatest impact on the organization. In fact, Enterprise Management Associates (EMA) estimates that, on average, more than 60 percent of all critical system and application outages are caused by inappropriate changes.

The costs associated with unplanned and uncontrolled change are significant and can impact an organization's customer service, security and compliance, and administration. Unplanned and uncontrolled change can lead to a longer time-to-value for new products and services, and can cause inconsistent and unpredictable service, which may force frustrated customers to go elsewhere. Uncontrolled change can also increase security and compliance risks, opening an infrastructure to malicious attacks and limiting an organization's ability to apply compliance strategies or the principles of good corporate governance. In particular, auditors are concerned that an organization can manage the change process, and evidence of uncontrolled change can lead to failed compliance audits.

Finally, uncontrolled change can increase administrative costs as systems fail to provide the level of service expected and IT teams are forced to duplicate efforts and repeat processes in an effort to ensure that things are done correctly.

Yet if nothing is allowed to change or evolve within an enterprise, an organization can fall behind as competitors take the lead in the market. The key is to implement processes and procedures to manage and control change.

Identifying Planned and Unplanned Change in the Infrastructure

By validating authorized changes and detecting unanticipated changes quickly, organizations can ensure quick problem resolution and control costs. A recent EMA study showed that, on average, problem resolution can take between one and four hours, with a significant part of the delay—between 30 minutes and two hours—dedicated to simply detecting and identifying the changes that caused the problem in the first place. Reducing this time is essential; in the time it takes to detect and resolve an issue, service and availability levels can be impacted and frustrated customers may already have given up.

There are a number of reasons that detecting change can be such a challenge. The first is the complexity of today's IT implementations. For example, a single server can contain thousands of configuration elements, including system files, kernel parameters, registry keys, application settings, and firmware switches, each of which must be optimized to meet IT business requirements. Since a typical organization may have tens or hundreds or even thousands of servers, the number of configurations to be tracked and managed can reach into the hundreds of thousands.

Network topologies—which must provide service to internal, remote, and outsourced workers, as well as to partner environments—have also grown more complex to meet business requirements for security, accessibility, and data sharing.

At the same time, the concept of a “distributed view” of IT components is complicated by the range of technology in heterogeneous environments; the differences in the scale of devices, which can extend from PDAs to mainframes; and the broad range of application types.

Unplanned and uncontrolled change can lead to a longer time-to-value for new products and services, and can cause inconsistent and unpredictable service, which may force frustrated customers to go elsewhere.

The complexity of IT infrastructures contributes significantly to another reason that detecting change can be such a challenge: an organization's lack visibility into change. Traditional methods of managing and monitoring change are impeded by IT staffs that simply don't have time or resources to look at each element of a complex infrastructure individually, or who lack information about critical configuration settings. The result is "configuration drift": configuration settings that have changed over time until they're far from what they're expected to be.

So how do most organizations detect unplanned change? In an EMA survey, 18 percent of respondents indicated that they learned about unplanned changes after an outage or slowdown and an additional 24 percent said they detected unplanned changes manually. (See Figure 1, below.) In both cases, it is likely that the organization was suffering adverse effects from the unplanned changes—particularly in terms of reduced availability and increased costs—before the problem was detected.

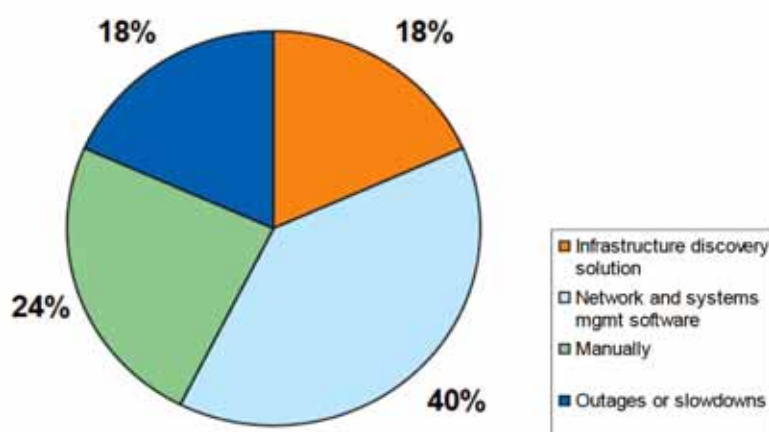


Figure 1. EMA Research asked survey respondents to identify the ways they learn about unplanned changes within their IT infrastructure.

Building a Change and Configuration Management Strategy

An effective change and configuration management (CCM) strategy ensures that control is maintained over an IT infrastructure. Change management is the process for identifying, authorizing, and implementing changes to IT components, and configuration management establishes and deploys appropriate IT settings. Configuration management is essential for ensuring that the right settings are in place to maintain uptime, availability and security. Configuration management can impact the configuration of servers and other assets, capacity planning, configuration of environments designed for business continuity, and application lifecycles across an environment.

Implementing automated CCM solutions enables organizations to meet business IT requirements with efficiency and cost effectiveness and to meet security, cost, and compliance requirements as well.

Configuration Management Primer

- Detect all change across the IT infrastructure independent of who made the change or why the change was made
- Reconcile actual changes based on acceptance criteria or with authorized change requests
- Report change activity and provide management with actionable information

Automation is critical. Given the complexity of today's IT infrastructures and the importance of visibility into change, it is simply not possible to manage change with manual processes. IT staffs do not have the time required to review configurations manually for change or to make sure that configurations are changing as they should. Plus, prompt problem resolution requires prompt problem identification. Attempting to address change and configuration issues manually can result in a high rate of downtime, increased cost, and decreased business productivity, which can threaten customer relationships and leave the organization open to compliance issues.

Implementing an Effective Automated Change and Configuration Management Solution

An automated change and configuration management solution must meet several key criteria to be successful. First, it should offer a single, centralized interface for identifying all configuration elements across an IT infrastructure. This centralized interface should provide timely change notification to enable a user to know when a change has occurred and provide the information necessary to take proper action to proactively eliminate potential problems.

An automated CCM solution should also deliver powerful reporting capabilities that provide a high-level status of overall enterprise health. (This is particularly important in a complex environment where it is essential to determine at a glance whether systems are secure, available, and compliant.) The reporting capability should also offer alerting of critical, unauthorized changes, especially those capable of triggering security breaches and intrusions, and should simplify methods of achieving compliance by providing the auditable evidence required to meet many regulations.

In addition, an automated CCM solution should provide an organization with a way to validate that changes have been made, closing the loop on the change request process. Implementation of a change, authorized or otherwise, does not ensure that change requirements have been met, so it is important to be able to validate that a change has actually occurred. For example, manual errors, faulty scripts, or the failure to follow established processes can prevent proper deployment of a change, and many tools, such as automated patch deployments and application upgrades, do not self-validate the success or appropriateness of their processes.

As is the case with security practices, validating a change event—whether a software upgrade, patch, configuration item change, etc.—must be performed independently from the change deployment mechanism to ensure consistency across your environment.

Integration with the Configuration Management Database

Today's successful IT service management implementations include the deployment of a Configuration Management Database (CMDB), an ITIL best practice.

The CMDB provides a central repository for a complete range of IT data, including configuration items and the software library, and it allows for a single point of access for IT governance, asset management, inventory, change and configuration management, and service assurance. In addition, the CMDB provides the integration point for many ITIL disciplines, including service management, release management, and problem management.

A recent EMA survey asked respondents to rate the advantages of a CMDB. 46 percent cited support for change management processes and the ability to know when and where change is taking place, whether configuration items conform with policies, etc.

A recent EMA survey asked respondents to rate the advantages of a CMDB (See Figure 2). Fifty-eight percent pointed to the capability of the CMDB to integrate data across multiple solutions, including patch management, software distribution, and change and configuration management. Nearly half of the respondents (46 percent) cited support for change management processes and the ability to know when and where change is taking place, whether configuration items conform with policies, etc.

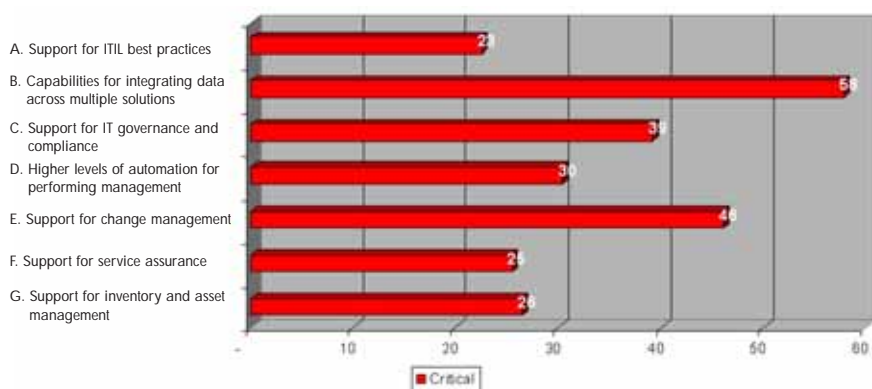


Figure 2. Respondents to a recent EMA survey identify their perceived advantages for implementing a CMDB.

Uncontrolled Change Increases Security Vulnerability

When it comes to protecting the enterprise against unauthorized change and malicious attacks, network security tools such as firewalls and anti-virus software are not enough. Security violations can occur from a number of unmonitored sources, including local network access, removable media such as CDs and DVDs, portable devices such as PDAs and flash drives, Internet downloads, remote file transfers such as those made through a VPN connection, and unauthorized access from hackers and other individuals with stolen or improper credentials.

These security violations can leave the door open for additional threats that are also unlikely to be detected by network security tools, including malicious damage by disgruntled employees, malware propagation, and the accidental weakening of security functionality.

Only by identifying and controlling change and integrating change and configuration management with traditional network security tools can an organization ensure comprehensive infrastructure security.

Change and Configuration Management's Role in Compliance

Change and configuration management can help an organization deliver the IT performance and data integrity needed to meet government and industry compliance mandates, accepted industry frameworks such as ITIL, business requirements, and licensing requirements, including those for software licenses.

Without automated CCM, achieving compliance can be especially challenging. It is nearly impossible to identify the specific areas in a complex IT infrastructure that are out of compliance, and frequently, IT staff must be redirected away from key business initiatives in order to prepare documentation for an upcoming compliance audit. Perhaps the greatest challenge, however, is the threat of fines and other penalties that are levied against organizations that are not able to meet compliance requirements. Auditors are increasingly

Without automated CCM, achieving compliance can be especially challenging.

aware that strong IT controls are predicated on strong change and security controls. As a result, they are requiring organizations to meet specific change control objectives, including reconciling detected changes with authorized change requests. To be successful, an organization has to start with a sound change and configuration management strategy that allows them to understand what changes have been made and how they align with authorized change requests. The implementation of an automated CCM solution will simplify this process by providing system-based validation of compliance.

Addressing Security and Compliance with Change and Configuration Management

In an EMA survey, nearly 100 percent of respondents indicated that a change and configuration management solution was either “critical” or “important” to ensuring security and compliance.

Change and configuration management unifies compliance and security to ensure strict control over critical IT infrastructures. With an automated CCM solution in place, organizations can maintain and enforce policy-based processes for change and provide policy-based controls to identify and remediate breaches. Plus, these solutions often provide verifiable audit and control of access and change across the infrastructure.

CCM reinforces appropriate data security by validating appropriate access rights are enforced across all IT assets, appropriate configuration controls are maintained, and the capability to identify and remediate any misconfigurations before data can be exploited.

Finally, CCM ensures security and compliance best practices for automated detection and remediation, compliance checking, and continuous compliance reporting.

Change and Configuration Management with Ecora Software

Ecora is a leader in enterprise-wide change and configuration reporting solutions that address a pervasive problem—the lack of visibility into configuration changes across the organization. Ecora’s Auditor Pro provides out-of-the-box policy and reporting functionality that enables organizations to resolve IT service management and compliance issues efficiently and effectively. Auditor Pro collects configuration data from across the infrastructure, including operating systems, database management systems, directory services, and applications, and presents reports customized for particular business needs using a centralized, web-based console. The detailed cross-platform configuration information captured by Ecora Auditor Professional can be federated into existing CMDB implementations, providing organizations expanded insight into their environments, providing additional value for their initial CMDB investment.

Ecora customers who automate the process of change management and reporting:

- Report 22 percent fewer trouble tickets over time
- Reduce the time spent resolving trouble tickets by 50 percent
- Increase efficiency through closed-loop change validation
- Prove regulatory compliance quickly, consistently and cost effectively

Keys to Meeting Compliance Demands

- Detect/collect/report configuration changes
- Reconcile changes against configuration “baseline”
- Reconcile changes against change management records
- Detect and remediate unauthorized changes
- Integrate changes with centralized CMDB

For example, Auditor Pro's Baseline Reports identify existing exceptions to any internal or external standard. Specific baseline reports might address improperly installed applications, unapproved service additions, GPO changes, or share NTFS permissions extended to a person without proper access rights. Change Reports identify changes between multiple points in time. These are invaluable for comparing a last known good state to the present state to identify the potential root cause of an outage. Among the things a change report might identify is a change in the Exchange protocol settings that is causing an email delivery problem, an error in the SQL tables that is preventing a finance database from being accessed, or a difference in patch levels between a production web server and a test web server that is causing some conflicts for visitors to the site.

ecora
Systems not running anti-virus software

-Prepared On: Thursday, February 22, 2007 12:00:39 PM

Service Name	Domain Server	Start Mode	Startup Acct.	Status
MSAfe Framework Service	BSR/VISTA1	Manual	LocalSystem	not running
Network Associates McShield	BSR/VISTA1	Automatic	LocalSystem	not running
	BSR/SQL_W0RK	Automatic	LocalSystem	not running
	ECU/MSF-PTS-000	Disabled	LocalSystem	not running
	ECORA/BUILD01	Automatic	LocalSystem	not running
	QAMINGE.LOCAL/HQ0100	Manual	LocalSystem	not running

Figure 3. Running anti-virus and anti-spyware software is a standard best practice to ensure security. Reports like this one can identify any systems that are not running appropriate security software and compare results to the organization's established policy requiring all systems to be running anti-virus and anti-spyware.

ecora
Disabled User Accounts

-Prepared On: Thursday, February 22, 2007 12:00:39 PM

Domain Name	User Name
BSR/SQL_W0RK	Guest
BSR/VISTA-AC1	Alones
	Guest
	LocalUser
ECU/PTS-001	Goldman
	Guest
	Little
ECORA/AF-W0RK	Guest
	Thacke
ECORA/ESH1	FThurans
	Guest
	Support
ECORA/PCI-W0RK	Standham
	Quems
	Guest
	Goodham
GA/ECORA/EXCH01BETA	ACalderin
	Richards

Figure 4. Reports such as this one validate that the accounts for terminated employees, temporary workers, or guest users have been disabled; allowing administrators to identify any gaps and take corrective action to mitigate identified risks.

If you implement processes and policies for sound configuration and change management, you will realize improved service delivery, reduced downtime, increased customer satisfaction, and a more profitable organization.

