



# Achieving Control: The Four Critical Success Factors of Change Management

Technology Concepts & Business Considerations

TECHNICAL WHITE PAPER

**Table of Contents**

Executive Summary ..... 3

Introduction ..... 3

    Audience ..... 3

Taking Charge: Beyond Basic Support ..... 4

An Opportunity for a Strategic IT ..... 4

Change Today: In a Vacuum ..... 5

A New Look at People, Processes and Tools ..... 5

    The Stakeholders: Unified Communication ..... 5

    The Processes: The Key to Control ..... 6

        Adding Six Sigma into the Mix ..... 6

    The Tools: Closing the Loop on Change ..... 7

    Taking Back Control ..... 7

Conclusion: The Complete Cycle of Change ..... 8

## Executive Summary

The goal of change management is to ensure that configuration changes (both planned and unplanned) are made cost-effectively, in a manner that enhances the delivery of service to the business, with the least amount of impact on the IT infrastructure.

Many organizations already have a handful of tools and processes in place that attempt to do this. However, for most companies, the processes are typically only documented on paper and there may be just a tool or two that addresses part of the change process, but not all of it.

This piecemeal and somewhat limited approach to managing change provides basic support as far as planning for and implementing expected changes, but it stops there. There are no means to validate that the change has occurred, no process to accommodate unexpected changes, and there isn't any way to identify the ramifications of the change on the IT infrastructure or the business. It's in this gap between the known and unknown where IT loses control and where security breaches, compliance infractions, and service outages occur.

## Introduction

Recently, EMC published a comprehensive guide for IT management entitled, *The Optimal State of Operational Excellence: The Six Best Practices of Configuration Management*. The best practices cited in this white paper included:

- End-to-end configuration and change management capabilities
- A holistic view of the enterprise and its configuration assets
- A proactive and continual approach to change and configuration
- Robust, integrated, and automated processes
- Actionable measurements
- Adaptive intelligence

The intention of this white paper is to delve deeper into the practice of change management and examine how this discipline contributes to an optimal state of operational excellence.

## Audience

This white paper is intended for IT and security professionals, compliance officers, auditors, process owners, and senior management.

## Taking Charge: Beyond Basic Support

In order to go beyond basic support and close the gap created by unknown changes, it is imperative to have a change management solution that supports the following four critical success factors:

### 1. Visibility: The awareness of what is changing

- Complete visibility into every planned change in the IT infrastructure, including in virtual environments

---

*“Broad configuration change detection capability is needed to guarantee system integrity by ensuring that all unauthorized changes are discovered (and potentially remediated).”*  
*“...there is a continued heightened awareness of security vulnerabilities, as well as an increase in the number of changes and types of changes being made across an IT infrastructure, which is now compelling IT organizations to implement mechanisms to track these changes to ensure that there is no negative impact on availability.”*  
*“Regulations do not provide a clear definition of what constitutes compliance for IT operations and production support, so businesses must select reasonable and appropriate controls, based on reasonably anticipated risks, and build a case that their controls are correct for their situation. Reducing unauthorized change is part of a good control environment.”*

— Gartner Group  
Hype Cycle for IT Operations Management  
July 2009

---

- Insight into whether additional incidents or ad-hoc changes occurred

### 2. Accountability: Responsibility for effective change

Verification that changes have been made

- Automatic identification and remediation of unplanned changes
- Validation or updating of security measures that ensure continued compliance

### 3. Measurement: How change affects the business

- Metrics and analytics of the impact on the business of the change

### 4. Improvement: Continual movement toward an optimal state of configuration

- Intelligence that measures processes in order to provide improvement of service
- The means to effectively plan for the next optimal configuration
- A full understanding of the cost of the change cycle

## An Opportunity for a Strategic IT

When control of the infrastructure is achieved through the implementation of the success factors above, the IT organization can contribute great value to the business through the delivery of leading-edge technologies and continual high-quality business services. And it is at this point where IT moves from being a cost center to a strategic partner that helps the company grow and become more competitive.

## Change Today: In a Vacuum

IT environments are becoming increasingly complex as organizations capitalize on the cost-saving benefits of cloud computing, virtualization, and other emerging trends. At the same time, the demands of the business are rapidly expanding, with more advanced technological solutions being introduced every day.

Given these parameters, change management becomes a difficult discipline to enforce, implement, and manage. Change often happens in a vacuum, with isolated incidences occurring with little (if any) knowledge or intelligence on how that change affected the business or the IT infrastructure.

For instance, many IT executives would have a hard time answering the following questions after a major configuration change, such as a significant patch on 1,000 machines.

- Was there any verification that this planned change was made accurately and that it was implemented on every applicable machine in the environment?
- Was there an accountability step built in, or did the same person who made the change close the ticket?
- Were there any unplanned incidents that were created as a result of the initial change? If so, how many occurred and where were they? Was additional remediation necessary? Were there any ad-hoc changes made? Was IT aware of them?
- Were there any unaccounted downtime or service interruptions? If so, how many users were impacted and for how long?
- What was the mean time to repair (MTTR)?
- What was the cost of the change? What was the cost for not only IT, but also the business as a whole, in specific areas such as customer loyalty and lost sales?
- Were the people responsible for security and compliance involved in the change? Were standards such as PCI compromised?
- How did the change affect any virtual infrastructures and DMZ environments?

After reviewing these questions, many IT executives quickly realize that they do not have the tools or processes in place that allow for them to really control and manage change within their environment.

For organizations that are ready to acknowledge this, it is time to take a closer look at what needs to be in place in order to have a truly effective change management solution.

## A New Look at People, Processes and Tools

At the heart of almost every effective technology solution is the right combination of people, processes, and tools. The same is true of change management—the most effective solutions require a strategic exchange of communication between the key stakeholders throughout the company, a solid framework of best-practice processes such as ITIL and Six Sigma, and a comprehensive set of end-to-end change management tools.

### The Stakeholders: Unified Communication

Change within an organization affects every part of it, from the top down, including corporate, everyday business operations, security and compliance, and IT operations. Too often, however, these functional areas operate as silos, without cohesive communication of the key business objectives that impact their operation and the business at large.

Best-in-class change management solutions solve this dilemma by involving stakeholders from each functional area in a platform such as a Change Advisory Board (CAB).

Through clearly defined roles and responsibilities that are aligned with the objectives of each group and the organization as a whole, a CAB engages the stakeholders in any change that is planned, helping to generate a greater understanding of the potential benefits (or pitfalls) of a proposed change on the business. For example,

by including security people on the CAB and holding them accountable for the company's governance, any vulnerability that might result in compromised compliance standards can be immediately remedied.

With an exchange of key information that is pertinent to the organization as a whole, IT can then build upon the next element of controlled change, a framework of processes.

### The Processes: The Key to Control

Within the change management cycle, it only takes the actions of one person who steps outside the parameters of an established process—whether as a reaction to an emergency change or an ad-hoc fix due to lack of time—for a failure to occur or for security to be breached. It's as simple as that.

Best-practice change management processes create a solid framework within which standardized policies, methods, and procedures can be established. These govern any configuration change, whether planned or unplanned, with delineated roles and responsibilities that provide rigorous accountability for every step.

Processes can be set up for the prioritization of how changes are managed, with repeatable processes that address everything from minor patches, to major upgrades, through to emergency outages and downtimes. This type of framework also allows for an operational structure for the CAB, review parameters for Requests for Change (RFCs), timeframe standards for change, and reports for management.

For organizations that are serious about implementing a robust change management solution, the adoption of IT Information Library (ITIL) processes is key.

As the most widely accepted IT service management (ITSM) framework of its kind, ITIL is an integrated set of best-practice recommendations with common definitions and terminology for not

*“The major benefits of leveraging ITIL are its structured approach to managing IT, the delivery of its services, and the introduction of a common language across the different domains or working groups.”*

Forrester Research,  
Why IT Service Management Should Matter to You,  
September, 2008

As Forrester Research notes, the adoption of processes such as ITIL helps an IT organization move from the role of “a technology silo into an organization that leverages processes to deliver IT services to its customers.”<sup>1</sup>

The implementation of ITIL processes has been increasing steadily, as organizations begin to realize the benefits of improved service levels and the reduction in the cost of IT operations.

### Adding Six Sigma into the Mix

To maximize the effectiveness of ITIL, many IT organizations are also employing Six Sigma strategies.

A quality management methodology first implemented by Motorola in the late 1980s, Six Sigma is a strategy that shares many of the objectives that are found in ITIL: process improvement, continuous process design and redesign, and process management.

With Six Sigma, the element of statistical measurement is introduced, which helps IT achieve greater acceptance and adherence to the ITIL processes. By following the practices of Six Sigma, IT can develop detailed policies and procedures, defining how to map, measure, and improve the quality process.

Together, ITIL and Six Sigma provide IT with a highly structured means of controlling change in the infrastructure while driving quality improvement and reducing operational costs.

---

<sup>1</sup> Forrester Research, Why IT Service Management Should Matter to You, September, 2008

### The Tools: Closing the Loop on Change

In order to have a successful change management solution, there is a need to monitor and measure its effectiveness and this is where the tools come in.

Best-in-class change management tools help IT to not only identify necessary changes, but also to minimize disruptions, remediate unexpected changes automatically, measure what has taken place, and report the results back to the business. This closed-loop capability gives control back to the IT organization, so that service is continually delivered and improved upon.

Here are the key tools that are necessary for controlled change:

- **A comprehensive CMDB.** The configuration management database (CMDB) is a centralized repository of key configuration items (CI), with broad coverage for applications, security settings, operating systems, and the ability to span and manage distributed IT services. Before, during, and after process changes through ITIL, the CMDB monitors the CIs within the enterprise, correlating all elements and attributes of configurations against policies. A best-in-class solution will even go one step further, identifying errors and vulnerabilities that occur even outside of ITIL-defined processes.
- **Change remediation.** Only a few change management solutions actually provide IT with automated change processes and workflows. This is an important capability that allows for the detection of any change from established baselines; it also allows for the automated reconciliation and verification of any operational configuration changes.
- **Configuration audit.** Many robust solutions include the ability to continually audit both expected and unexpected change in an IT environment, with the goal of providing a baseline of configuration standards for a desired state and ensured system integrity. With an automated, continuous auditing process, ITIL and Six Sigma standards can be enforced across the enterprise with relatively little effort. IT can then identify critical trends that affect both current and future performance, and track performance against desired objectives.
- **Security and compliance.** The best solutions on the market will also come with rigorous security, regulatory, and operational compliance configuration settings that are defined by industry best practices and guidelines. These solutions automatically create, distribute, test, and enforce the security policies required by audits, regulatory acts, and international standards.
- **Analytics.** It is critical to know what is and is not working in the IT environment. By transforming vast amounts of siloed information into actionable insight via key performance indicators and business objectives, a mature change management solution can help IT focus on increasing the quality of service while managing a highly adaptive, intelligent, and optimized organization.

These tools can be integrated with ITIL and Six Sigma processes to dramatically improve the change management process and help an organization be much more effective and in control.

### Taking Back Control

With the right communication, processes, and tools in place, the critical success factors of visibility, accountability, measurement, and improvement work together in concert to give IT complete control of the change management process.

Here's an actual example of a situation where a proper process was not in place, and how the incident could have been avoided with the right change management solution.

- A large financial institution recently purchased a new software package that was designed to help make the lending process easier for both the institution's employees and its customers.
- During the installation of the software, the IT department – which was not asked to participate in the evaluation or the purchase of the package – was instructed to leave the database administrator's password blank in order for the software to interface with other parts of the solution, such as the ATM and online services.

- Because of this oversight, the organization later lost critical customer data, including Social Security numbers and credit card data, due to a security breach. Because of this incident, the institution's integrity was compromised, customer loyalty decreased, and there were substantial financial ramifications as well.

Here is how this would have evolved if the right change management process—and the four critical success factors—were in place:

- With a CAB in place to review proposed changes, IT would have had visibility into the evaluation process and been involved in each stage of the purchasing process.
- Accountability would have been established with the vendor for any associated risk to the software, as well as with the institution's security and compliance personnel.
- The effect of the installation on the business would have been measured, including the occurrence of things such as downtime, resulting incidents, and any required remediation.
- There would have been continual improvements to the overall security and compliance posture of the organization and with customer service via the upfront establishment of both business and IT goals. Any required processes and tools would have been implemented to support the continued meeting of compliance standards such as PCI.

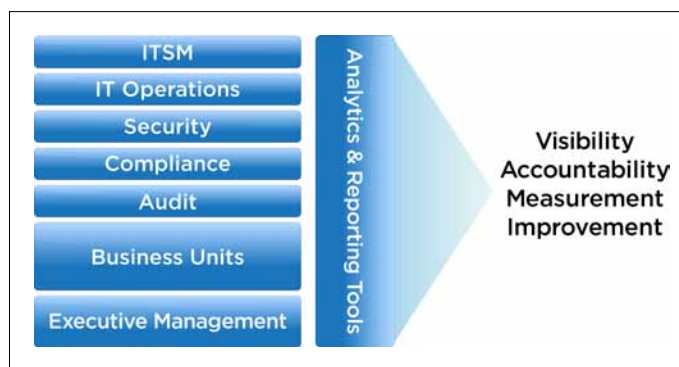


Figure 1: Change management across the stack

## Conclusion: The Complete Cycle of Change

When organizations have complete visibility into change, they know what to expect, they discover the unexpected, and they are able to remediate quickly, either rolling back the environment to a secure configuration, or moving it forward to its next desired state.

With this added visibility, IT organizations can now understand who is making what change with accountability that eliminates unexpected changes that cause service outages and costly mistakes. Moving to the next step of this closed-loop process, IT executives can then measure the impact of the change in relation to the business objectives and corresponding security and compliance requirements.

And finally, IT organizations can get even better at what they do best: bringing the organization to the next level of optimal performance, delivering better services, and driving cost efficiency throughout all levels of operation.

---

*User Advice: "Develop sound configuration practices in your organization before introducing configuration auditing technology. Greater benefits can be achieved if robust change management processes are also implemented. Process development and technology deployment should focus on the systems that are material to the compliance issue being solved..."*

— Gartner Group  
Hype Cycle for IT Operations Management  
July 2009

---

