WHITE paper

Enforcing IT Change Management Policy

"Everything flows, nothing stands still." —Heraclitus

The Greeks knew long ago that it is impossible to step into the same river twice. Fast-forward from ancient Greece to our technology-driven century, and change occurs so rapidly it is difficult to manage. Managing change is one of the most difficult challenges that IT organizations face, and to effectively support and facilitate enterprise business goals, IT must also continually change. Sometimes these changes are significant, as in upgrading a network. Some changes are almost imperceptible, occurring without fanfare as services evolve and underlying IT infrastructure is maintained.

Infrastructure Complexity Magnifies the Impact of Change

While planned, authorized changes have obvious benefits to systems or users, unknown and even imperceptible changes can result in serious negative impact to IT systems and processes. IT organizations are responsible for a complex structure of "systems of systems," all of which must work together to deliver quality information and communication services. Each "service" requires a specific, integrated "stack" of systems—such as applications, databases, middleware, directory services, operating systems, and networks—in order to successfully deliver a set of functions or processes. The unique behavior and state of each system in a stack is determined by a multitude of elements, such as file systems and their attributes, configuration settings, users, and permissions.

This complexity means that changes in the IT infrastructure can potentially affect every part of a business operation, posing various degrees of risk to the enterprise. For example, an unauthorized change to firewall settings can result in serious vulnerabilities that not only threaten data and disrupts revenue-generating services, but that can also imperil compliance with regulatory requirements.

Instilling Change Controls

Change must be controlled to mitigate the inherent risk to IT's compliance, service quality, and security posture. Indeed, national and local laws, as well as private contractual arrangements, demand that organizations deploy effective controls on their IT infrastructures. One form of control is developing change management processes. These processes are often based on best practices, such as the IT Infrastructure Library (ITIL), and supported by an array of system management techniques, tools, procedures, and policies that together help define the organization's change management process.

Having processes in place is not enough, however. Change management policies and controls must be systematically evaluated and enforced. If they are not, companies experience:

- Control deficiencies that can result in poor audit findings, potential fines, and other disciplinary measures
- Difficulty and higher costs to prepare for audits
- Service outages, unplanned work, and delayed delivery of strategic projects resulting from unauthorized and undocumented changes
- Increased risk and security vulnerabilities
- A lack of assurance about system security and data integrity

How High-performing Organizations Manage Change

Companies that successfully embrace change management gain at least three significant benefits:

- They spend less than 5 percent of IT time on unplanned work (also known as firefighting)
- They experience a low number of "emergency" changes
- They successfully implement desired changes more than 99 percent of the time, and experience no outages or episodes of unplanned work following a newly implemented change.

How do organizations become high performers? According to the Institute of Internal Auditors' Global Technology Audit Guide, *Change and Patch Management Controls,* these organizations have fostered a culture of change management that prevents and deters unauthorized change.

Culture

In a change management culture, IT staff adhere to change policies and processes because managing change has become a strategic value, or part of the "DNA" of that IT organization. This culture starts at the top, with executives who understand that unauthorized change constitutes uncontrolled business risk. They not only expect policies to be followed—they inspect processes to ensure that they are followed. "Trust but verify" is the mantra of top performers.

Top management must provide clear, consistent communication that sets expectations that change management must be followed. And they support that posture by ensuring that change policies are in place and enforced.

Controls

Control over IT is achieved by instituting effective policies, then implementing robust controls to ensure that all changes are auditable and authorized, and that all unauthorized changes are investigated. Organizations with weak IT controls invariably spend a higher percentage of their resources on unplanned work, while producing sub-standard operational results and delivering inferior service to their customers.

Credibility

Credibility cannot be implemented—it must be earned. IT organizations achieve credibility when they demonstrate control of IT and can document a history of consistent accountability, applied consequences, and measurable improvements. When people circumvent proper procedures, they are held accountable and experience tangible consequences for evading the system.

Organizational change is never implemented without resistance. While many IT staff members commonly protest that increased change controls will slow them down as they perform their tasks, high-performing IT organizations consistently prove that implementing good processes and controls actually increases efficiency and productivity throughout the organization.

Maturing IT Processes

What determines if an IT organization is a high performer or if there is room for improvement in its change management processes? The amount of time spent in firefighting is one of the most obvious indicators. In the average IT organization, it is common for unplanned tactical responses to take significant amounts of time away from strategic projects. Implementing and enforcing effective change policies will reduce firefighting and free resources for initiatives and projects that are aligned with the enterprise's business goals.

Tripwire, together with the IT Process Institute (ITPI), has been studying customers and world-class IT organizations for several years. To better understand commonalities between top-performing IT organizations and provide a prescriptive approach for improving service management, Tripwire has identified four capability levels of maturity in change management processes.

Level 1: Reactive

IT groups in this first level typically spend most of their time fire-fighting and have problems with poor service levels and long outage times. There are usually few formal processes established, almost no systematic communication about changes happening in the environment, and an abundance of finger-pointing about the causes of service interruptions.

Level 2: Using the Honor System

As their users and management become increasingly dissatisfied with downtime, poor service quality, and a lack of strategic development, IT organizations begin implementing a defined change management process.

They begin to document policies and practices, and start to put technologies in place to try to guide the change authorization process, relying on the "Honor System" for ensuring that individuals adhere to the new policies and procedures. Organizations often become frustrated, because they cannot systematically determine when people circumvent these new policies.

Level 3: Using Closed-Loop Change Management

When organizations deploy closed-loop change management processes, they begin to realize significant performance gains. Closed-loop change management exists when detective controls are deployed for detecting changes to production infrastructure, and all changes are reconciled with authorizations to ensure that no undocumented or unauthorized changes escape notice.

At this stage, there is typically a formal project or strong executive sponsorship to resolve change management process issues and to bring service levels and IT costs under control. With executive support and appropriate controls, service levels improve markedly and unplanned work dramatically declines.

Level 4: Continuously Improving

Once they have experienced the benefits of closed-loop change management, companies begin to use their newly acquired control to pinpoint problems and inefficiencies. They are then able to systematically attack and improve weak areas, which enables continuous and ongoing improvement. Companies at this level, while not perfect, are able to provide predictable, high-quality services in a cost-effective manner.

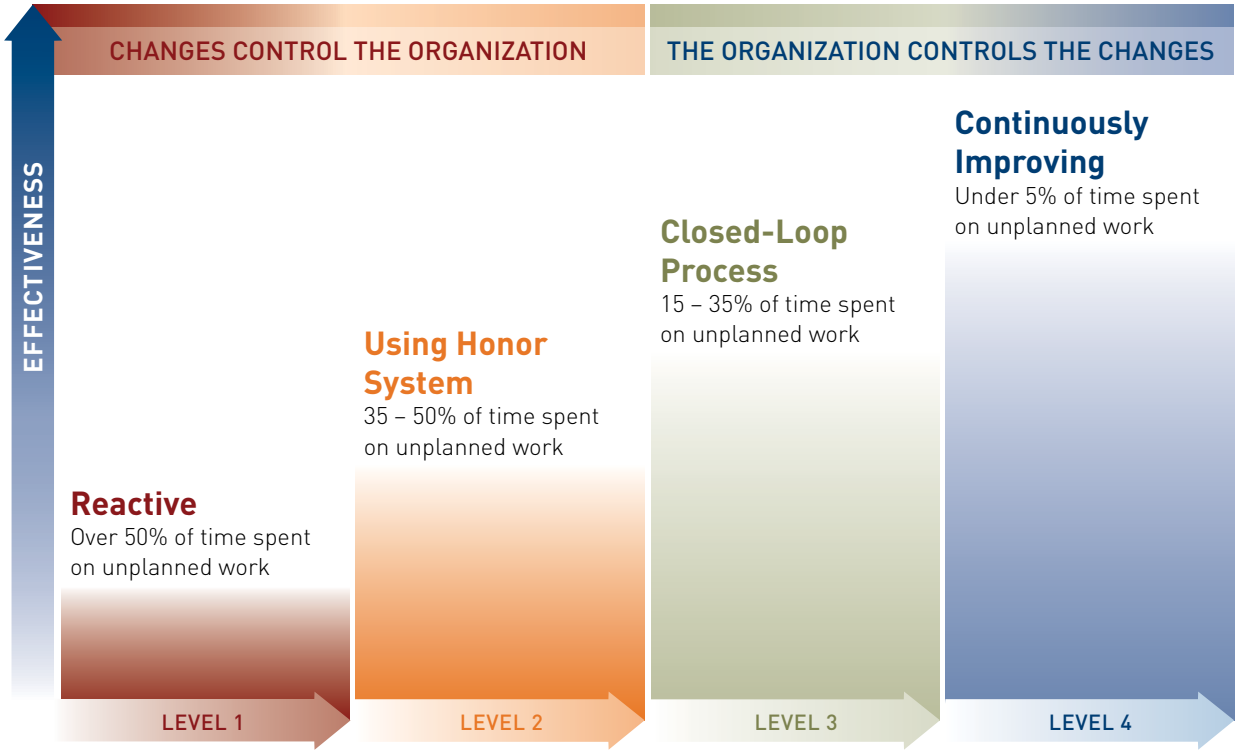


Figure 1: The Four Levels of IT Maturation

Organizations interested in implementing a change management program must first identify their current level of maturity and define their desire change management goals. Questions that can help determine the present level of IT maturity include:

- What is the overall goal of the change management process?
- What percentage of their time does the IT staff spend on unplanned work?
- If something changed in the IT environment, how would anyone know?
- What is the volume of emergency changes in the IT environment?
- Is the change audit trail properly documented?
- How many failed changes have been experienced and what were their causes?

Enforcing Change Policy

Controlling IT requires controlling change—which requires change policies enforced by effective controls to ensure that all changes are auditable and authorized and that all unauthorized changes are investigated. For change policy enforcement to work on a practical level the following requirements must be adopted.

All Changes Must Be Auditable

All IT infrastructure changes and changes to all service stacks must be audited, made clearly visible, and documented. Because each service is comprised of complex systems, as previously described, IT must be able to monitor high rates of change to high-risk systems and introduce policy changes that will reduce or eliminate episodes of unplanned work.

Someone other than the person or technology authorized to make changes must approve and record each change. By segregating these duties, IT can prevent fraudulent change recording and mistakes made through over-familiarity with specific systems. Finally, a historical audit trail describing all changes, including when they were made, and by whom, must be maintained. Organizations must master basic control objectives before they can take on more advanced challenges.

Basic Control Objectives

- All production devices must be monitored for changes
- All changes to high-risk systems—referred to as "fragile artifacts" in the Visible Ops methodology—must be recorded, explained, and documented
- A baseline of configuration items is retained as a reference check point
- Change implementers can not authorize their own changes

Advanced Control Objectives
These include the above and:

- All changes must be tested in pre-production before being implemented in the production environment
- All production changes must be recorded, explained, and documented
- Change verification and validation should be performed after implementation
- Emergency changes should include an adequate audit trail to allow tracking from incident to underlying cause and back
- Change successes and failures should be tracked

All Changes Must Be Authorized

Unauthorized change is the primary cause of unplanned work, unanticipated downtime, and business risk. Only authorized changes are acceptable. An authorized change that corresponds to an established change policy may require that a trusted person make the change and only during a scheduled maintenance window. It may also require that a change exactly matches both the change previously approved in the quality assurance environment and an approved change ticket.

Basic Control Objectives

- The Change Advisory Board must review all changes
- All devices in production must be scanned for change at pre-determined intervals
- No changes to production assets are allowed outside scheduled maintenance windows
- All changes must map to an authorization ticket

Advanced Control Objectives
These include the above and:

- No changes will be made to production assets except by specific roles and individuals
- Change implementers will not authorize change requests, nor approve completed changes
- No changes to production assets are allowed by pre-production personnel

All Unauthorized Change Must Be Investigated

Each detected change must be mapped to authorized work orders or flagged for investigation—unauthorized changes cannot be ignored. The change may be a malicious act, but more often it is the result of mistakes made by authorized individuals. Regardless, detected, unauthorized changes must be investigated to determine if they should be accepted or rolled back to a previously known, good state. It may be prudent to treat high-severity unauthorized changes as security breaches until proven otherwise. Controls should be in place to make certain that unauthorized changes are resolved quickly. A detection system is critical to the organization's ability to implement effective change controls.

Control Objectives

- All unauthorized changes must be escalated, investigated, documented and resolved within a specified timeframe
- No unauthorized change should remain in the environment

Tripwire Facilitates Change Management

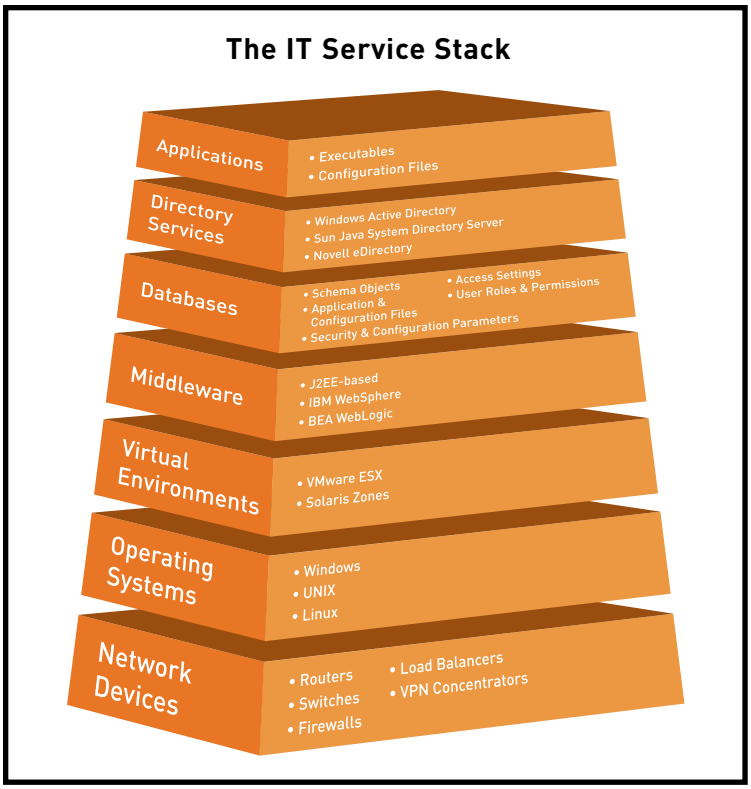
Gaining control of IT requires an effective combination of people, processes, and technology. Business process owners, IT staff, security personnel, and auditors must work together to define and enforce change policies and processes. Once policies and processes are defined, they can be enforced with technology.

Tripwire Enterprise configuration audit and control software supports change control and a culture of change management by detecting, reconciling, and reporting changes to information infrastructure systems. With Tripwire Enterprise, IT management and auditors have proof that all changes are auditable, all changes are authorized, and any unauthorized changes that occur are investigated.

Tripwire Professional Services provide expert knowledge to help IT organizations evaluate their current maturity level, define change policies, and implement effective change control processes in their unique IT environments. With effective controls and expert assistance, IT organizations can deploy highly effective change management processes that facilitate audit readiness, help achieve compliance goals, improve service quality, and assure the integrity of their IT infrastructures.

Change Detection So That Every Change is Auditable

Tripwire Enterprise provides an independent, single point of management control for enterprise-wide change monitoring of IT systems, including directory servers, file servers, desktops, databases, middleware applications, and a broad range of network devices, including network switched, routers, firewalls, and Virtual Private Network (VPN) systems. Within these systems, Tripwire monitors elements of the service stack—such as file systems and their attributes, configuration settings, users, and permissions—even across service stacks comprised of systems from a variety of vendors.



Tripwire detects change relative to a specific, trusted state known as a baseline, against which any change is automatically compared and logged, ensuring that every change is auditable. Only users with appropriate permissions are able to accept detected changes and include them in the current baseline if the changes are desired and authorized, further enhancing auditability. Tripwire Enterprise can also independently verify that desired changes were made successfully—whether they are implemented with IT management and administration tools or by direct human intervention.

Organizations with numerous systems can easily monitor their infrastructures with Tripwire, reducing the administrative burden associated with monitoring thousands of heterogeneous devices, multiple operating environments, and multiple vendors' equipment. Infrastructure nodes can be grouped into logical, user-defined groups with configurable severity levels to denote the relative significance of a change that can trigger different response actions.

Change Reconciliation Ensures All Changes are Authorized

Determining which of an IT organization's thousands of changes are authorized—and which are not—is a task for technology. Tripwire's change reconciliation capabilities enable IT organizations to institute a variety of manual and automated techniques to identify appropriate changes and unauthorized changes that may negatively affect enterprise compliance, security, or service quality.

Detailed change information enables IT to quickly ascertain:

- Who made the change
- When the change occurred relative to scheduled maintenance windows
- Whether the change matches a change previously detected and approved in a QA environment
- Whether the change corresponds with an approved change ticket.

By delivering detailed change information to the appropriate staff members, Tripwire Enterprise allows them to match approved, expected changes with actual changes—to validate authorized upgrades or releases. Integration with change ticketing systems can automate the reconciliation process, triggering appropriate actions when change is detected. Actions can include sending alerts and change detail to approved staff using email or SNMP, as well as triggering commands that can be used to run predetermined tasks or activate third-party tools, such as system backup tools.

Reconciliation also accelerates identification of unauthorized changes and facilitates investigation of these changes. Tripwire Enterprise configuration audit and control solutions help IT management define change processes, enforce them, and document when these processes are circumvented so that the enterprise can reduce risk, avoiding negative consequences, and increase operational efficiency and availability.

Change Reporting Substantiates Change Policy Effectiveness

Tripwire Enterprise provides a wide range of customizable reports and online dashboards to highlight changes across the enterprise. With report linking, managers can drill down into underlying details and metrics. For example, a report could illustrate the change rate of selected systems for the past year; a manager could drill down to view changes for a specific quarter, month, or week. Real-time status reports facilitate incident management and help staff determine outage root causes. Reports and dashboards can be archived for future reference in HTML, PDF, or XML formats.

Tripwire reporting features deliver high visibility into operations, enable IT to foster process improvement and integrate configuration audit and control capabilities with security, compliance, and system availability initiatives.

Why Change Control is Worth It

Fostering a culture of change and enforcing change management processes pays off in greater auditability, improved service quality, and IT infrastructure integrity.

Configuration audit and control reduces the cost and difficulty usually associated with audit preparation and makes it easier to pass internal and external audits. For example, Sarbanes-Oxley requires completeness and accuracy of financial reporting. The Payment Card Industry (PCI) standard requires protection of cardholder information. If all authorized system changes can be documented, once configured, tested, and deployed into production, they will continue to operate appropriately unless changed.

Configuration audit and control also improves service quality and reduces unplanned work, breaking the chronic emergency environment and firefighting that consumes many IT organizations. By reducing unplanned work, IT systems become more predictable, delivering highly reliable services and enabling IT staff to focus resources on new services that can be deployed on time and within budget.

Strong internal change controls provide management and auditors the confidence and supporting evidence that security measures are effective and IT systems operate with integrity. They mitigate the risk of malicious changes and provide security staff with a reliable, objective view of change across an enterprise.

In the 21st-century IT organization, change management is more than just a good idea; it is required to meet business objectives successfully. By creating a culture of change, implementing effective controls, and earning credibility from enforcing policies, IT organizations can achieve the title of a high performer—from an objective process perspective and in the eyes of the users they serve.

tripwire™
www.tripwire.com
US TOLL FREE: 1.800.TRIPWIRE **MAIN:** 503.276.7500 **FAX:** 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA