



WHITE PAPER

Proving Control of the Infrastructure

The need for independent detective controls within
Change/Configuration Management

Gene Kim, CTO, Tripwire, Inc.

Rob Warmack, Senior Director of Product Strategy, Tripwire, Inc.

- page **2** Getting Control
- page **3** The Control Triad: Preventive, Detective and Corrective
- page **5** Defining Automated Change Auditing
- page **6** An Automated Change Auditing Solution
- page **7** Proof Positive



Proving Control of the Infrastructure

The need for independent detective controls within Change/Configuration Management

Gene Kim, CTO, Tripwire, Inc.

Rob Warmack, Senior Director of Product Strategy, Tripwire, Inc.

In virtually every industry, the success of an organization is inextricably linked to the reliability, availability and security of its Information Technology (IT). Consequently, IT management must identify and analyze the relevant risks facing its production environment and then put controls in place to prevent, detect and correct for them. Not only are these controls required for effective management, they are also good for business and fundamental to meeting regulatory compliance requirements.

Unauthorized access due to security breaches is a high-profile risk. Hackers from outside the network, or more likely, employees or contractors with means, motive and opportunity, manage to bypass or defeat security defenses and make malicious changes to software files and system configurations. These unauthorized changes can have dire consequences, such as financial loss, disruptions to IT operations, and negative public perception.

Although security often gets the spotlight, the much greater risks to the organization are system reliability and availability issues. Gartner asserts that “80 percent of unplanned downtime is caused by people and process issues, including poor change management practices, while the remainder is caused by technology failures and disasters.”¹ IDC cites similar findings that indicate that operator error is the single largest source of outages causing nearly 60 percent of overall infrastructure downtime.² Many IT organizations, in the spirit of being nimble and responsive to their customers, are actually putting themselves at risk in the everyday process of making changes to their own systems.

If industry analysts are correct, and practical experience certainly indicates that they are, the greatest point of leverage for increasing the overall reliability, availability and security of information systems, and addressing related compliance requirements, is controlling change across the IT infrastructure.

Getting Control

IT management has tried many things to control change. They have invested in a variety of change and configuration management (C/CM) products or developed their own sets of tools to manage infrastructure changes. They have improved the efficiency and speed of the C/CM process, such as automating the change approval process workflow, automating the deployment of software and configuration changes, as well as automating the discovery of information assets and mapping these assets to the services they provide.

¹ Donna Scott, VP and Research Director, “Best Practices for Operational Change Management,” Gartner, Inc. 2003

² Stephen Elliot, IDC, Senior Analyst Network and Service Management, 2004

Despite all this technology and automation, reliability, availability and security issues still exist and proving compliance remains difficult. Consider the case of patch management technologies that inadvertently result in servers that will never boot again, all deployed at speeds never possible without automation. The mistaken assumption is that by automating and systemizing the way change is authorized and implemented, human error is also reduced. All too often, these tools don't actually improve service quality and can even exacerbate the situation by enabling more undesired changes to be made more frequently.

Why is it essential that changes to IT infrastructure be controlled? First, IT risks create real business risks because the most critical business processes are often run entirely on IT. Second, effective management of IT hinges on the effective management of IT infrastructure—you cannot manage the IT service or IT value without first effectively managing the IT infrastructure. IT infrastructure spans all the servers, network devices, and databases that IT application services are built upon, as well as the controls that protect them, such as firewalls and intrusion detections systems.

Integrity of the IT infrastructure is foundational. Like a building built on unstable ground, when the integrity of the IT infrastructure lacks stability, reliability or security, the integrity of the entire system dependent upon that infrastructure, and perhaps even the entire organization, is not stable, reliable or secure.

But why has change management failed for some organizations and flourished in others? Two industry organizations, the Software Engineering Institute and the IT Process Institute, have been studying IT organizations that have demonstrated superior levels of availability with the greatest efficiencies, the lowest amount of unplanned work, and the best security process integration. Their change volumes are among the highest—and yet, they enjoy the highest change success rates.

What makes these high performing IT organizations successful is that they have a culture of change management with effective controls in place that *enforce* the change management process. They also have a culture of causality that ensures that change is ruled out first in the repair cycle.³ Like any operation striving for high quality, high-performers detect production variances early, before they cause downtime or a security event, and evaluate their performance based on defined metrics. They, too, have made varying degrees of investment in automated C/CM tools, but the difference is that the high performers have also implemented effective processes and controls that continually assess the effectiveness and efficiency of their change management processes.

Without such controls, IT organizations lack an effective, proactive way to quickly discover when the wrong change was made, or when the right change was made but at the wrong time.

The Control Triad: Preventive, Detective and Corrective

Driven by Sarbanes-Oxley legislation and a growing list of other regulations, IT management is quickly coming to appreciate both the importance of internal process control to the organization at the highest levels, as well as the significant effort required to continually prove that internal process controls are both in place and effective.

³ "Best in Class Security and Operations Round Table Report," Software Engineering Institute/Carnegie Mellon University, 2004.

Likewise, the audit industry is working to provide IT management open control frameworks, such as Control Objectives for Information and related Technology (COBIT) and ISO17799, to help identify, document and evaluate IT controls.

In the language of audit, high performing IT organizations must have internal process controls to mitigate the inherent risks of change. Internal process controls are policies, procedures, and practices put in place to ensure that business objectives are achieved and risk mitigation strategies are carried out.⁴

According to the Institute of Internal Auditors, there are three categories of internal process controls, all of which are relevant to change management:

- *Preventive Controls* – controls that define the roles and responsibilities, processes, and policies intended to manage change management risks;
- *Detective Controls* – controls that automatically track and reconcile production changes, and detect when preventive controls fail, and;
- *Corrective Controls* – controls that review change implementations and provide recovery mechanisms to mitigate the impact of failed changes.

These three controls are independent of one another and must provide verifiable evidence proving that not only that each control exists, but that the controls are effective against identified risks.⁵

Though IT organizations vary in sophistication, most are likely to have some preventive controls in place to define change management and security policies. For instance, they may have policies that require changes to be formally requested, approved and tested before deployment. From a security perspective, effective perimeter defenses and identity management tools and technologies are expected to be in place to maintain a defensible barrier around the network.

However, merely having preventive controls is not enough: Organizations with just preventive controls still have unscheduled and protracted downtime, low change success rates and high levels of unplanned work. This shows that preventive controls alone are not adequate for reducing change and security-related business risks.

Without the balance and enforcement of a detective control, preventive processes are easily circumvented or simply ignored. Unintended and unauthorized changes made to production infrastructure go unchecked and often result in unplanned downtime. Likewise, it is possible for malicious changes to either penetrate the security perimeter or originate from within the organization unnoticed to only be discovered after IT service is impacted. And if a failure in a preventive control goes undetected, corrective actions aren't likely to be triggered until the failure becomes visible throughout the organization.

A detective control serves as a *tripwire* that discovers the failure or circumvention of preventive controls and alerts IT or triggers associated processes to take corrective action. To be effective against the increasing volume of changes, a detective control must cover the breadth of the infrastructure and independently discover change made by any source. By reconciling desired changes and exposing those that are undesired, an effective detective control automatically audits change and provides IT managers and auditors comprehensive, meaningful reports of change activity.

⁴ "IT Control Objectives for Sarbanes-Oxley," IT Governance Institute, 2004

⁵ "Change and Patch Management: Critical for Organizational Success," Institute of Internal Auditors, 2005

Defining Automated Change Auditing

Change auditing isn't a new concept. Manual inspections and custom scripts are commonly used to verify that changes are made correctly. However, several trends create very real challenges for IT: the growing volume of changes driven by the business, the increased rate of change driven by automated change deployment technologies (e.g., patch management and software distribution), and the inability to manually reconcile these changes to authorized work orders. Consequently, the majority of changes—and the integrity of the change management process—is simply assumed to be properly managed.

To auditors and a growing number of IT executives, “management by good intentions” is unacceptable. On-the-fly modifications, work-arounds, and untested quick fixes eventually take their toll as system configurations drift slowly away from a known and trusted state and processes break down from a lack of enforcement. The price is paid later when unexplained outages result after patches fail or servers can't be quickly rebuilt, and unplanned work is required to resolve the issues. More and more time is spent on rework and unplanned work, detracting from completion of planned work.

The solution is automated change auditing, simultaneously addressing reliability, availability and security, which has three critical functions within the C/CM process:

- independent detection of change regardless of source or intent
- reconciliation of detected change with intended and authorized change
- independent reporting of all change activity across production systems

Independent change detection: The fundamental role of change auditing is to serve as an independent detective control with the ability to automatically detect system changes across an entire infrastructure comprised of a disparate, far-flung mix of servers, routers, firewalls, databases, etc.

As an independent detective control properly segregated from the persons or technologies making the changes, the change auditing system detects changes regardless of who made the change or why the change was made. This means capturing automated and manual changes, authorized and intended changes, as well as the occasional unauthorized, unintended, or potentially malicious change, in sufficient detail to determine the date, time, implementer, system, and the details of the change made.⁶

Detecting change at this level requires first maintaining a baseline for each system to define a known and trusted state of software files and configurations, and then continually checking all systems to discover when deviations from baselines occur. By logging and accepting only those changes that are authorized and intended, IT management has continual proof that the integrity of the infrastructure is intact.

Change reconciliation: The majority of infrastructure changes are authorized and intended and must be independently validated to prove that desired changes occur as planned. But more importantly, desired changes must be resolved and filtered out to uncover any undesired changes. If a change can't be correlated back to change approval or release management processes, preventive controls have been compromised and corrective controls must be triggered.

⁶ “Change and Patch Management: Critical for Organizational Success,” Institute of Internal Auditors, 2005.

Integration with other C/CM tools enables the change auditing system to automatically correlate detected changes with approved intentions and trigger recovery whenever necessary. Change ticketing systems define which changes are approved, may describe the intended changes, as well as indicate when the changes should be made and by whom. Within release management, software distribution or configuration management tools can also define what changes were expected to be deployed. When undesired change is detected, the change auditing system must alert appropriate systems and network monitoring tools, plus open incident tickets within the service desk so the undesired change can be further explored. For practicality and usability within an enterprise, it is essential that the change auditing system be highly scalable, centralized and offers sufficient interfaces to facilitate these various integrations.

Independent reporting: A change auditing system provides IT management and auditors proof of systems and process integrity by generating an independent accounting of actual changes across the breadth of the infrastructure, reconciled with authorized and intended changes. These reports offer ongoing proof that effective change controls are in place, as well as provide decision support tools for problem management.

Complementing what a change ticketing or configuration management tool can provide, a change auditing system provides an independent, verifiable audit log of all actual change activity, not just planned changes.

Performance indicators generated by change auditing can serve as IT operational metrics, as well as security and assurance metrics, reporting:

- the number of actual changes made to the IT infrastructure;
- the number of those changes that were authorized;
- the variance between planned and actual changes, and;
- where the most frequent changes are being made and who is making them.⁷

Change activity reports are also essential as decision support tools when restoring service interruptions and outages, and resolving service incidents and problems. Change auditing information can be used to determine if change was a causal factor to an incident or problem. If changes are discovered, the detailed change information can be used to establish when the system was last in a known and trusted state, then identify exactly what changed from that baseline, when it changed, and even who made the change.

An Automated Change Auditing Solution

Other C/CM products offer pieces of a change auditing solution, but lack the comprehensive capabilities previously described that are essential to an effective independent detective control.

- Change ticketing systems are aware of authorized changes, but can't automatically determine if its approved changes are ever actually made.
- Software distribution and patch management tools understand the intended changes they are instructed to deploy, but ignore those changes that occur outside of their defined scope of responsibility and cannot deal effectively with manual or scripted changes.

⁷ "Change and Patch Management: Critical for Organizational Success," Institute of Internal Auditors, 2005.

- Server and network configuration management tools are limited to the domains they manage (e.g., just servers or network devices) and aren't able to automatically reconcile with other C/CM systems the changes that they may detect, nor report on the effectiveness of the overall change management process for the infrastructure.

Tripwire provides change auditing solutions that specifically address the enterprise's need for independent detective controls. Its solutions provide a single point of control for detecting, reconciling and reporting change activity across servers, workstations, network devices, and a growing number of other infrastructure components. Its library of graphical reports and executive dashboards document detailed change activity and provide essential change performance indicators. This information enables IT management to better manage change and the overall integrity of the infrastructure, and therefore IT as a whole.

Proof Positive

Change auditing assures compliance by demonstrating that internal control structures for change management and security are in place and effective. When combined with a change approval process that allows only approved and tested changes to be implemented, change auditing increases the availability of information systems both through enforcement of better change management processes *and* by offering decision support tools to quickly remediate outages and incidents when they inevitably occur. Finally, change auditing enhances security and instills greater confidence in IT systems by demonstrating that only authorized and intended changes have been made to the production environment. These capabilities demonstrate that an independent change auditing solution is essential for proving control—as well as systems and process integrity—across the IT infrastructure.

To Learn More

For additional information on change and configuration management and change auditing solutions as they relate to IT auditing, regulatory compliance, the IIA and GTAG, best practices such as ITIL/Visible Ops and COBIT, the ITPI and the ITGI, please visit www.tripwire.com/solutions.



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