IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Configuration and Change Management for IT Compliance and Risk Management: The Tripwire Approach

Sponsored by: Tripwire

Frederick W. Broussard Vivian Tero

November 2007

EXECUTIVE SUMMARY

Increasingly, IT departments are regarded as service providers to end users. Thus, IT departments must manage their hardware and software assets with the objective of providing efficient customer service to all constituents. Service provision requires that IT identify specific sets of services (such as in a service catalog), identify the assets required to deliver the services, authorize users to access the services, and establish processes and best practices for service delivery on an ongoing basis.

The need for effective processes for service delivery has resulted in the increasing adoption of best practices based on IT Infrastructure Library (ITIL), ISO 20000, Six Sigma, and other process standards and frameworks. Indeed, these best practices are being adopted worldwide by IT departments that wish to improve customer service to both internal and external customers. These standards help streamline and standardize internal IT processes, resulting in higher IT efficiency and improved service delivery to end users. One of the most critical areas that need strong operational processes is managing changes to the IT infrastructure. This includes processes for management of authorized and planned changes as well as facilities for detecting and preventing unauthorized changes.

What is needed is a streamlined, integrated approach to managing change that incorporates hardware and software asset discovery, discovers relationships between assets, and ensures that approved hardware and software asset configurations are maintained intact and are not corrupted by accidental or unauthorized changes. This is a key foundation for meeting a variety of regulatory compliance requirements. Tripwire has developed solutions that address this need, and when integrated with other solutions for discovery, these offerings can provide the necessary configuration and change management for multiple types of IT environments. IDC recommends that IT managers consider Tripwire solutions to support these functions.

IN THIS WHITE PAPER

This IDC White Paper discusses key issues surrounding configuration management and compliance. These issues center on the IT department's need to lower costs, increase management flexibility and control, and increase responsiveness to business needs and requirements. Managing change and satisfying compliance requirements are critical parts of the IT department's service delivery mission. Accidental or unplanned changes to the IT configuration, or configuration settings that "drift away" from standards, can have drastic consequences in terms of

service disruption for the business as a whole. IT organizations need software solutions that can address the need to effectively manage and control changes to configuration settings.

SITUATION OVERVIEW

Change is intrinsic to any business. Technology innovation, evolving customer preferences and requirements, disruptions in the supply chain, and regulatory developments are market forces that demand that businesses adapt quickly to these shifts and be able to innovate. IDC's January 2007 *QuickLook Survey* of senior business and IT executives underscores this business sentiment. The results show that the top 5 business initiatives leading the CEO's agenda are (in order of highest to lowest frequency rates):

- Customer care and service enhancement
- Product (or service) innovation/development
- Sales productivity/performance improvement
- Regulatory compliance
- Business performance monitoring

IT organizations must have the ability to effectively manage their IT assets and changes to the IT infrastructure to enable the business to respond to market developments in a timely fashion. For compliance and risk management purposes, IT should be able to support these responses in a consistent and auditable fashion, and with minimal risk of business disruption. The survey data suggests that senior IT executives are aware of these needs. Among senior IT executives, the top 3 priorities are product (or service) innovation/development, regulatory compliance, and IT organization responsiveness and efficiency improvement.

From an IT standpoint, the overarching theme among these CEO priorities is obvious. Businesses want to have a flexible and resilient IT infrastructure that would allow them to quickly adapt to and take advantage of developments in their business landscape. Senior business and IT executives also increasingly recognize that these business priorities do not exist in a vacuum and converge with critical functional areas within the enterprise. IT organizations today recognize that the ability to manage IT assets and the configuration and change processes is central to enabling operational effectiveness.

IT departments must address the needs of the business unit in managing change. In some organizations, this means moving away from the perception of IT as a cost center focused on technology to the perception of IT as a business partner adding value to the organization. Part of this changing need centers on the ability of the IT department to reconfigure its hardware and software quickly to meet business needs and changing requirements.

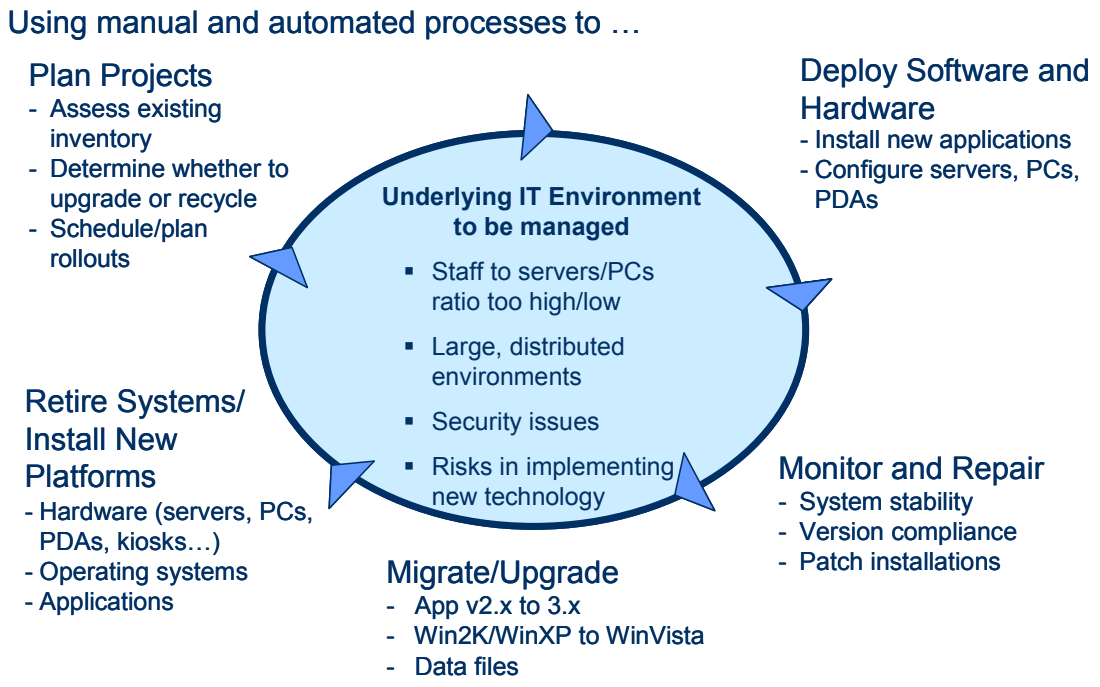
Current Practices in IT Change Management

IT organizations often use software solutions that focus on one specific area relative to infrastructure management. Such solutions, sometimes known as point products, have advantages of being relatively cheap to acquire and effective for a specific area of function or individual pain point. For example, IT asset management software can address identifying and inventorying the computers attached to the IT department network and recording their hardware and software configurations. Such tools, however, lack the capability to enforce standards for configuration settings or ensure that machines are denied network access if they do not comply with a required configuration in the first place. Similarly, patch management solutions may address only vulnerability assessment and distribution and discovery inventory functions.

Life-cycle management practices are generally required when using any software solution to manage hardware and software assets. IT organizations have been using point solutions as well as integrated product solutions to manage across the life cycle. See Figure 1 for more details.

FIGURE 1

Life-Cycle Management



Source: IDC, 2007

Managing server hardware and software assets, as well as databases, Web servers, virtualization, network devices, and applications, requires a focused approach to configuration and change management. This includes managing the existing configurations of these systems and processes and knowledge for their continued maintenance and eventual retirement. This is also the same for the company's desktop and laptop PCs as they move through a typical three- to five-year life cycle. Representative tasks are to keep applications up to date with the latest versions, ensure that necessary patches have been installed, and migrate to the next version of the operating environment when required. All of these tasks need to be performed with an eye toward ensuring that the underlying configuration is compliant and meets the objectives of the business service for internal and external customers.

At the same time, an eye needs to be kept on the continued enforcement of approved configuration settings, as both intended and accidental changes can be introduced into the approved configuration. Further, because specific tasks, functions, and personnel form part of a compliance chain within the approved configuration, any changes to that configuration must also be managed to ensure continuous compliance with the appropriate regulations and policies.

Solutions available from a number of vendors help manage necessary software changes and updates to the configuration, but there needs to be a "smart" way to manage change and verify that changes comply with appropriate regulations and that changes continue to be auditable.

Managing Change for Continuous and Operational Compliance

In the IDC 2005 multiclient study *Priorities for Corporate Compliance*, businesses indicated their intent to leverage and extend their existing siloed compliance IT investments to support multiregulatory requirements. The Sarbanes-Oxley Act of 2002 (SOX) imposed sweeping changes to a publicly listed organization's business and IT operations. In the run-up to the SOX deadlines, businesses focused on the documentation of critical business and IT processes as well as on the identification and remediation of material weaknesses in these processes.

In 2006, the IDC survey *Information Management for Compliance* suggested that there was a broad consensus among businesses that the first two years of SOX compliance were largely inefficient. Businesses reported that the projected declines in the ongoing cost to comply with SOX did not materialize. There were calls for the Public Company Accounting Oversight Board (PCAOB) to address what businesses derisively referred to as the "SOX Tax." Businesses' inability to intelligently audit configuration changes in the infrastructure and to dynamically invoke the appropriate actions often led to redundant remediation activities and hyperenforcement. Companies were caught in a vicious circle of chasing compliance requirements.

Today, businesses continue to seek opportunities to reduce the ongoing cost of complying with regulations such as SOX and at the same time respond to increased incidences of HIPAA audits and address new regulations around data privacy and legal discovery. The PCI Data Security Standard (PCI DSS), like SOX and Basel II,

can be particularly onerous for unprepared organizations. Visa's PCI Compliance Acceleration Program will charge noncompliant Level 1 and Level 2 companies higher commission rates on their transactions in addition to the monthly fines. These monetary penalties have a direct negative impact on the income statements of retailers and merchants. PCI DSS impacts transactional networks, systems, databases, and applications and demands real-time visibility into the changes in the IT infrastructure. Detecting and reporting unauthorized changes will not suffice. In fact, the regulation specifically states that all changes must be reconciled and unauthorized changes must be investigated.

Regulations such as PCI DSS, SOX, and Basel II demand that businesses be able to continually monitor and evaluate configuration activities and changes and dynamically take actions to enforce compliance to their desired state (i.e., create and enforce a state of continuous compliance for critical dynamic systems and IT processes). The benefits of continuous compliance would come from few incidences of audit failure, the ability to identify overlapping requirements and risk controls across multiple regulations and risk management policies (requiring fewer manpower and IT resources), and a reduction in potential challenges to existing practices that comes from having consistent auditable change control operations. Continuous change auditing and configuration assessment can also be employed to enable the IT organization to maintain its service-level objectives, mitigate outages in the datacenter, and address potential attacks to critical transactional systems.

Embedding the risk management and governance discipline in the configuration and change management processes could eventually position the business to mitigate risk from noncompliance and also enable efficiencies in the IT operations that would allow the business to effectively respond to changing market conditions to pursue new revenue and market opportunities. This state of operational efficiency would be analogous to the "real-time" supply chain.

Foundations for Enabling Continuous and Operational Compliance

For the majority of companies, the implementation and the operationalization of compliance and risk management objectives have posed the biggest hurdles. IDC research shows that the following processes, best-practices frameworks, and automation tools are critical foundations to move businesses toward the path of achieving continuous operational compliance.

CobiT

To achieve operational compliance, businesses have to enforce a disciplined approach to creating the linkages between their strategic business objectives, business processes, organizational culture, and IT operations. Businesses have adopted the CobiT framework to facilitate their SOX compliance efforts. CobiT organizes IT activities into generally accepted process models, identifies the categories of major IT resources, and defines the management control objectives that firms should consider. CobiT therefore provides a framework that allows businesses to create linkages between business objectives and IT objectives, create metrics and maturity models for benchmarking themselves relative to their industry peers, and

define the responsibilities of business and IT process owners. CobiT also enables businesses to identify areas of individual and functional accountability, which in turn, facilitates organizational issues around stakeholder buy-in, user adoption, and organizational change management. For SOX compliance, 12 IT control objectives were mapped to the PCAOB Auditing Standard No. 2 and CobiT processes. At a high level, these control objectives are:

1. Acquire and maintain application software
2. Acquire and maintain technology infrastructure
3. Enable IT operations
4. Install and accredit solutions and changes
5. Manage changes
6. Define and manage service levels
7. Manage third-party services
8. Ensure systems security
9. Manage the configuration
10. Manage problems and incidents
11. Manage data
12. Manage the physical environments

At a tactical level, these control objectives can also be applied and extended to functional areas and processes within the organization, specific to a regulation or the corporate IT risk management and governance policy. Managing change is highlighted as a distinct control objective (#5), yet change management issues encompass all these risk and control areas. For many IT organizations, the operational challenges come from (1) managing and optimizing the change processes so that they are prioritized according to business needs and are compliant with formalized security and IT operations policies and (2) having the correct and timely documentation to meet regular multiple audit requirements.

ITIL/CMDB/Best Practices

Whereas CobiT focuses on defining controls, IT process standards such as ITIL/ITSM and ISO 17789/20001 provide the structure that enables companies to execute their CobiT control objectives within IT operations in a consistent manner. Several businesses have adopted the ITIL process standards to implement and operationalize their defined control objectives. ITIL's focus on system management and a process approach to managing infrastructure helps streamline change management across the IT infrastructure, from the desktop to the datacenter. Central to meeting this need is the creation of a configuration management database (CMDB) that provides organizations with a repository for information about IT assets and configurations.

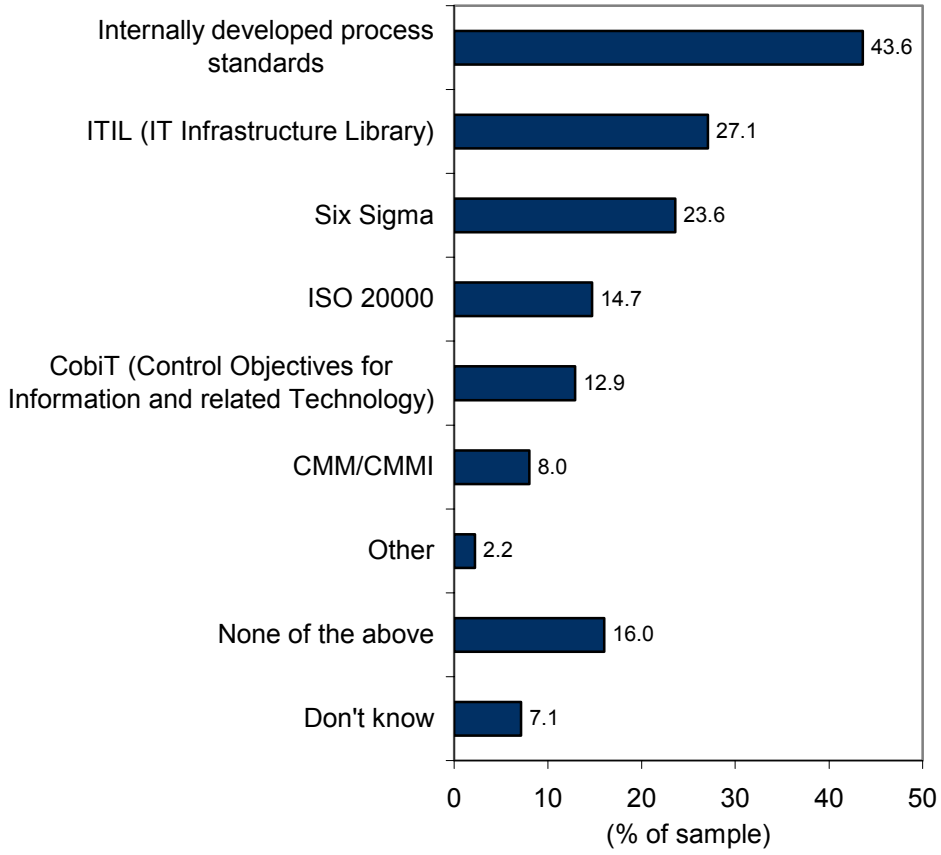
The CMDB gives IT organizations the ability to create and standardize hardware and software asset information across the entire company. It can therefore be used to develop baselines for operational performance and form the starting point for continuous improvement of IT infrastructure to meet business needs.

In February 2007, IDC conducted a survey of IT organization practices in using process standards and frameworks. This data shows that IT organizations are using not only ITIL to help manage their IT environments but other frameworks as well. See Figure 2 for more details.

FIGURE 2

Adoption of IT Process Standards and Best Practices

Q. Which of the following IT process standards or best practices (if any) is your organization using to manage at least one of your internal IT processes or workflows?



n = 225

Note: Multiple responses were allowed.

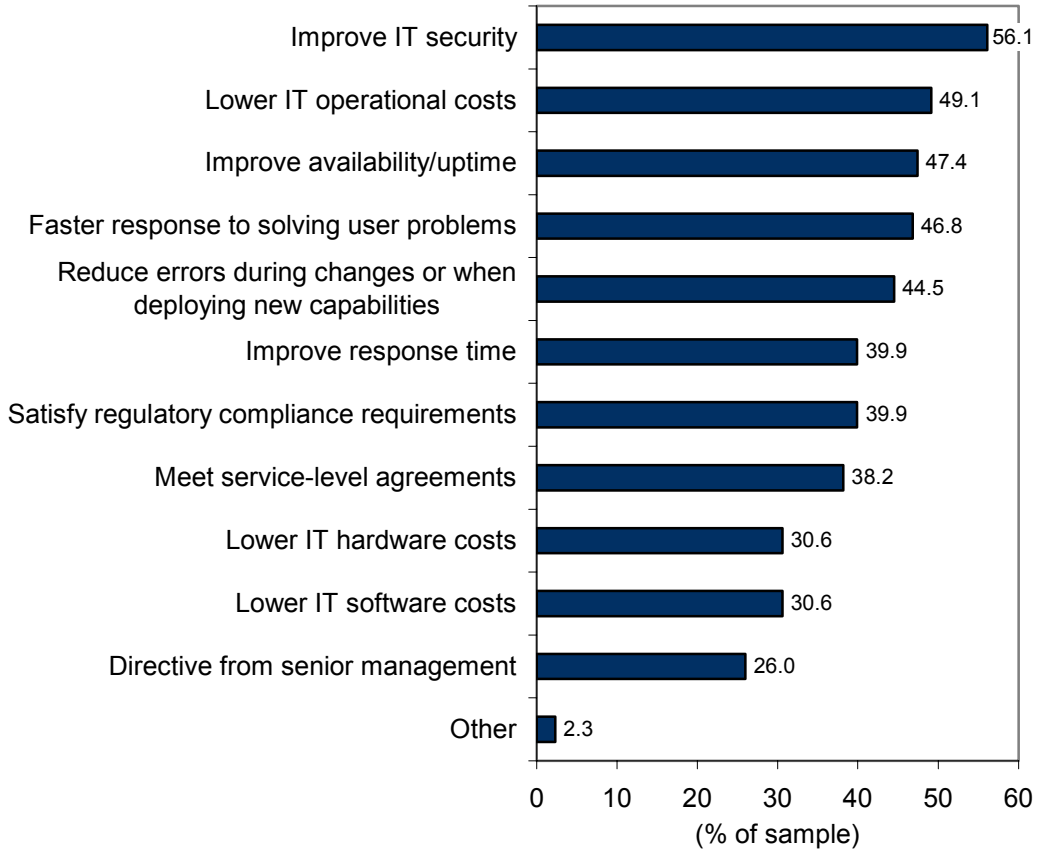
Source: IDC, 2007

This survey allowed respondents to provide multiple responses to individual questions. When respondents were asked which IT process standards they were using, 43.6% said they were using internally developed standards, 27.1% said they were using ITIL, and 23.6% said they were using Six Sigma. Overall, more than 75% of respondents said they were using an IT process standard within their organizations. Only 16% are not using any type of process standard. And when asked to identify the major drivers behind the adoption, 56.1% of respondents answered that improving IT security was a major driver. See Figure 3 for more details.

FIGURE 3

Drivers for Adoption of IT Process Standards and Best Practices

Q. What were the major drivers for your organization in the decision to adopt an IT process standard or best-practice approach to management?



n = 173

Note: Multiple responses were allowed.

Source: IDC, 2007

Another major driver in this survey was the need to lower IT operational costs, cited by 49.1% of respondents. Satisfying regulatory compliance requirements was cited by 39.9% of respondents as a driver for adopting an IT process standard. Because of the life-cycle nature of change and configuration management within the enterprise, IT departments may not be aware that by taking an integrated approach to configuration compliance (i.e., constantly managing changes to the environment so that these changes comply with existing regulations and procedures and are auditable), they will also be able to lower overall costs by building such features into their solutions. Therefore, IT departments are able to effectively manage IT operations in compliance with operational, regulatory, and security policies with fewer resources and less investment.

IT departments are following best practices when they take a sustainable approach to compliance, viewing it as a part of a continuous management approach to application, hardware, and software configuration management. Continuous compliance is a necessary competency to ensure success of IT department initiatives on behalf of business unit customers and the company as a whole.

As part of the ITIL process standard, the CMDB takes a much greater role in helping manage the IT department's assets. Functioning as the repository for configuration item (CI) information in the IT department, the CMDB is a key part of ITIL and service management.

As ITIL and other process standards gain traction within the enterprise, the CMDB will increase in importance. But the following software-based issues will have to be addressed:

- Architecture and design issues
- Need for open, nonproprietary access and interoperability
- Need for data visibility, such as with dashboards and reports

IDC also interviewed 25 IT organizations for data regarding the frequency of changes made and found the following:

- 40% of the changes are made to the server infrastructure (211 changes per month)
- 35% of the changes are made to the application infrastructure (185 changes per month)
- 25% of the changes are made to the network infrastructure (132 changes per month)

For more information, see *CMDB Deployments and Change Management: Efficiency Benchmarks for IT Organizations*, IDC #205371, January 2007.

As the CMDB is deployed and updated with CI information, the information in the CMDB will change over time as CIs are added, changed, or removed. Under the best of circumstances, the changes are known and approved. Frequently, as unapproved changes are made, either intentionally or accidentally, they affect the accuracy and integrity of the CMDB and can lead to the IT department's failing to meet business unit needs.

For example, a retail grocery store may have inventory of cereals, produce, medications, and meat and dairy products at the start of the year. The formal log-in of produce, meat, dairy, and other related grocery items happens as the products are delivered to the appropriate department and when they are purchased by customers at the checkout counter. The store management then knows what products are selling. But management does not know how well the products are selling or what products are not selling. So if shoplifters steal produce or produce goes bad and is discarded without logging the removal into inventory, then key items may not be available for sale, and revenue opportunities are lost.

Importance of Change History

Because CIs change over time, documenting CI changes becomes important to ensure the following:

- **Auditability.** The process of tracking and managing the changes occurring to CIs leads to ensuring that configuration audits can be accurately and quickly conducted. Thus, improvements can be controlled and managed with good information as a result of the audit.

- **Relationship traceability within the CMDB.** Information about a change to a CI is as important as the CI itself. The CMDB is more than a repository of configuration items; it contains the relationships between CIs, as well as information about specific releases, incidents, problems, known errors, and changes affecting the overall IT system. This requires the CMDB to be constantly updated to ensure that impacts resulting from changes are traced to the appropriate change.

The key is to have automated discovery and inventory of network, software, and hardware assets tracked at the appropriate CI level within the IT department and to ensure that the CIs are verified at all times. This will help ensure that unintended and unreported changes to those CIs are prevented and that existing approved changes are being enforced.

Businesses that have adopted the CobiT process models and ITIL best practices and deployed a CMDB are in a strong position to mature from a reactive "chasing compliance" mentality to a risk-based and governance approach. There are immediate tactical benefits to this approach. By automating the workflows between the policy and control objectives and performance metrics for critical processes, and between the testing and audit, remediation, and reporting of incidents and activities related to these processes, business and IT process owners are freed up from having to manually conduct these repetitive risk and control activities. Automation also allows organizations to provide an auditable chain of custody across the life cycle of an

incident and demonstrate consistency in its IT activities. Unplanned incidents and human error are difficult to predict and control. But having the ability to demonstrate and provide documentation on IT process consistency when responding to these events would make life easier when the auditors and regulators come knocking!

The risk-based and governance approach creates an IT organization where compliance and risk awareness become inherent to the IT organization's operational DNA. Doing so would allow the IT organization to move closer to a state of operational compliance.

Tripwire Inc.

Tripwire Inc. has made a name for itself focusing on integrated configuration, compliance, and audit control. The company was founded in 1997 with a focus on providing security solutions to IT departments. As ITIL increased in importance, Tripwire led efforts in that area by broadening its offerings to include managing IT operations within an ITIL context. Tripwire has grown to offer more than eight solutions that range from security and configuration management to regulatory and operational compliance. The company's solutions focus on the following areas:

- **Continuous operational compliance.** Tripwire solutions ensure compliance of internal processes, policies, and standards. For example, Tripwire ensures the accuracy and integrity of the CMDB to stay current with unintended and unreported changes, as well as approved changes, providing detailed change history to the CI. By achieving and maintaining compliance with operational processes and tools, Tripwire increases operational efficiencies and reduces business risk.

- **Continuous regulatory compliance.** Tripwire solutions ensure compliance with regulatory requirements such as PCI, SOX, HIPAA, FISMA, and many others to help reduce the cost and effort of demonstrating compliance to external constituents. For example, SOX requires CEOs and CFOs to be held responsible for the accuracy of financial statements. Tripwire assists in this critical function by automating the enforcement of change and configuration management processes and reducing audit costs by continuously demonstrating proof of compliance.

- **Continuous security compliance.** Tripwire solutions ensure security compliance by preventing unauthorized changes and configuration settings that violate security settings. For example, PCI DSS requires that companies keep credit card data secure and notify consumers when breaches occur. Tripwire provides a sustainable approach to PCI compliance by delivering an automated, holistic view of compliance across the IT infrastructure. This reduces security vulnerabilities and risks while effectively improving the services the company delivers to businesses.

Tripwire Enterprise

Forward-thinking business leaders in IT ensure that their organizations control risk and cost while simultaneously increasing operational efficiencies through process automation. Given that today's organizations exist in an environment where a data security breach or improperly executed system change can expose critical customer data or cause severe service outages, these IT leaders must take a deliberate approach to developing and controlling operational processes, policies, and standards across their enterprise. By quickly detecting and remediating issues generated by unauthorized or unplanned change, IT leaders can consistently deliver quality services to the business. High-performing organizations minimize risk associated with change by deploying configuration audit and control processes and tools throughout the IT enterprise.

Tripwire Enterprise delivers immediate value to the business by providing continuous operational, regulatory, and security compliance and ensuring that organizations achieve and maintain a known, trusted, and compliant state. Tripwire Enterprise delivers value in three steps:

- **Configuration assessment.** Tripwire Enterprise proactively assesses current configuration settings against established internal policies and external industry benchmarks. The assessment produces an enterprisewide risk profile that allows organizations to continuously address vulnerabilities one by one across the datacenter until the organizations move into a known, trusted, and compliant state.

- **Detect all change.** Once organizations achieve a known good state, Tripwire Enterprise helps them maintain it. Tripwire Enterprise detects all change across the entire IT infrastructure — applications, databases, servers, active directories, virtual environments, middleware, and network devices — and alerts IT to any unauthorized or noncompliant change.

- **Take action.** When Tripwire Enterprise detects unauthorized or unplanned change, it goes into action, generating detailed reports through the reporting console, automatically reconciling the change with leading enterprise management systems and CMDBs to trigger change remediation.

FUTURE OUTLOOK

IT departments are facing a number of trends that involve configuration and change management over the next 18–24 months. These trends include:

- **ITIL penetration.** ITIL is one of many process standards/frameworks being implemented to streamline IT operations. IDC research points to significant ITIL penetration within North America and the United States. This penetration is strongest within organizations that have more than 10,000 employees. These organizations are typically responsible for large datacenters that need to automate and streamline operations to ensure effective SLA execution, positive ROI, and smoother operations within the IT department as well as the business unit.

- **Multiple repositories supporting a CMDB.** Most organizations have one or more repositories of hardware and software asset information. With the adoption of ITIL, consolidation of these multiple sources into a manageable "federation" of sources will elevate the CMDB from merely a repository of basic asset information to a central focal point for managing change and predicting change impacts throughout the IT department. To do this, IT departments need solutions that perform all aspects of the consolidation: the initial asset discovery and inventory; the relationship mapping between assets, applications, and the network; and the reconciliation and enforcement of IT policies for managing change within the network. Consolidating this information into a single console provides the IT department the streamlined view needed for actionable information.

- **Increased virtualization use.** Server virtualization led to server consolidation, and this consolidation provides significant savings for datacenters. The net result is that CIOs and senior IT managers are left with a more complex IT environment in which physical hardware and software assets must be managed along with the virtual hardware and software assets. The complexity increases with each instance of virtual hardware and software that is created and removed because of workload requirements. Therefore, the number of changes to be tracked increases significantly if the management plans don't take into account virtualization within the datacenter.

- **Windows Vista and Windows Server 2008 migrations.** The release of Microsoft's Windows Vista operating environment and the rollout of Windows Server 2008 will force IT organizations to plan for the streamlined adoption of these operating environments within their IT environments. This presents a great challenge and a great opportunity for IT departments to plan for implementing and managing change. Previous Microsoft operating system releases have served other IT departments as a framework to consider increasing automation. This has meant, in many cases, an increase in cost. But this increase is usually justified by the installation of new software that increases system ROI as well as helps with the operating system rollout and migration.

CHALLENGES/OPPORTUNITIES

While Tripwire continues improving and updating its solutions and focusing on delivering business-relevant continuous compliance solutions, the company continues to face a number of challenges, including the following:

- As a growing company, Tripwire needs to continue to raise its market and brand profile. The company has developed a strong set of partners, most notably a channel relationship with BMC, and stronger integrations with HP's and CA's CMDBs. Tripwire has to continue selecting the features and functions that best meet customers' needs in order to continue its strong growth.

- Tripwire needs to ensure that it offers features addressing further policy discovery that augment available enterprise hardware and software solutions. These features must be continually updated to make sure that they work with the latest applications.

The company also has opportunities, such as:

- Further leveraging its relationships for the channel
- Penetrating an attractive niche within the compliance area that continues driving revenue growth
- Capitalizing on Windows Vista and Windows Server 2008 migrations (Microsoft's release of these operating environments also presents Tripwire with the opportunity to partner with Microsoft or other vendors in ensuring smoother rollouts. The configuration compliance experiences of customers that have already rolled out Tripwire Enterprise should help other IT departments in rolling out the new operating environments.)

CONCLUSION

ITIL, ISO 20000, CobiT, and Six Sigma are just a few of the process standards and frameworks that IT organizations use to manage change processes within their organizations. The large size of these organizations, their datacenters, and the mission-critical nature of the transactions they support require IT leaders and administrators to ensure that changes affecting the IT infrastructure "do no harm" as well as improve business unit and customer performance. This focus on ensuring that changes occur in the prescribed manner is especially important because of the regulatory climate.

Software solutions are available that help IT departments manage thousands of changes that occur within the datacenter over a year. But what is needed is a streamlined, standardized process that automates making changes, verifies those changes, ensures those changes are consistent with existing policies, prevents unauthorized changes, and provides auditable results.

Tripwire addresses this need. Tripwire Enterprise ensures continuous compliance by identifying authorized and unauthorized changes within the datacenter. IT departments that need to ensure that they are aware of authorized as well as unauthorized changes should strongly consider Tripwire Enterprise for their organizations.