



Reducing the Cost and Complexity of IT Management

White Paper

By Dan Sullivan, Realtime Publishers

January 13, 2006

COPYRIGHT

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Altiris and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION, INCLUDING WITHOUT LIMITATION ITS AFFILIATES AND SUBSIDIARIES, SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation," as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display, or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>

Altiris, Inc.
588 W. 400 S.
Lindon, UT 84042
<http://www.altiris.com>

CONTENTS

Reducing the Cost and Complexity of IT Management..... 1

- The Dynamics of IT 1
 - Business Drivers 1
 - Current State of IT 2
- Managing Change 3
 - Need for Visibility and Control 4
 - Maintaining Cost-Effective Controls 5
 - Breadth of Change Management 6
- Effective Change Management Requirements 6
- Summary 7



REDUCING THE COST AND COMPLEXITY OF IT MANAGEMENT

It is essential that the goals and operations of IT align with business strategies.

Information technology (IT) is a crucial factor in reducing costs and adapting to evolving market demands. At the same time, IT incurs costs of its own. One of the most pervasive but commonly underestimated costs is that of managing change. To manage the complexity of change in today's IT environments, it is important to understand the business and technical drivers behind that complexity as well as the tools available to address those needs.

The Dynamics of IT

The dynamics of IT and their effects on business are realized through a confluence of business drivers acting on the current state of IT within an organization.

Business Drivers

Business needs drive IT and four common drivers to IT deployments include:

- Aligning IT with business
- Standardizing systems management
- Maintaining compliance
- Ensuring a secure environment

It is essential that the goals and operations of IT align with business strategies. In today's markets—characterized by global competition, rapid communications, and streamlined production and supply chain operations—firms operate under constant pressure to reduce costs. At the same time, IT enables businesses to reengineer processes and deploy new products and services to meet the competing demands for reduced costs and improved quality.

To remain competitive and agile, baseline operations, such as systems management, must be streamlined. System updates, software patches, help desk services, and related activities are essential elements of IT, and therefore, business operations.

Another key business driver of IT is regulatory compliance. High-profile financial scandals of the last decade coupled with growing concerns over privacy protections have led to significant government intervention. Regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the European Privacy Directives have become common subjects in business discussions. Both financial integrity and privacy regulations place significant demands on information systems.

A growing area of concern among IT professionals is the need to maintain secure computing environments. Viruses, worms, and other types of malware threaten desktops, servers, and increasingly, mobile

devices. Effective security depends upon a firm understanding of one's infrastructure, configurations, and revision levels.

For example, the infamous SQL Slammer worm that disrupted Internet services in 2003 proliferated rapidly because so many administrators had not installed a patch for the vulnerability exploited by the worm. Compounding the problem was the fact that the Microsoft SQL Server Desktop Engine, a reduced function version of SQL Server, was widely distributed with other applications. This version was also vulnerable to SQL Slammer, but because the database was embedded within others programs, many users were not aware that they were running it, let alone needed to patch it.

The combination of market drivers, evolving regulations, and ever-present security threats create a constantly changing IT environment. Within this dynamic environment, some broad patterns have emerged across organizations.

Current State of IT

IT departments across industries share several common attributes that influence which services they provide and how cost effectively those services are provided. Some of the more dominant themes found today are:

- Heterogeneous environments
- Emerging technologies
- Outsourcing, consolidation, and other organizational changes
- Multiple compliance regimes
- Budget constraints

No single platform meets the needs of midsized or larger organizations. Desktops run end-user versions of Windows (and now Linux), and servers depend on UNIX or enterprise-scale Windows and Linux editions. Even when systems administrators diligently try to enforce standards, application dependencies can introduce conflicts.

For example, database administrators may decide that all Oracle servers will run a particular version of Linux. An upgrade to the company's enterprise resource planning (ERP) system, which runs on Oracle, may require another version of Linux due to a difference in system libraries. The business requirements for the upgrade rightly trump the desire to maintain consistent operating system (OS) platforms. The result, however, is a more complex environment that demands greater control.

Early adopter status can yield substantial benefits to businesses that can effectively introduce new technologies. At the same time, emerging technologies bring with them multiple types of risks, including disruption

to existing environments. They also introduce new change management challenges that may not be fully understood when acquiring new technologies.

Outsourcing has emerged as a viable model for delivering IT services. Outsourcing offers two distinct benefits: reduced cost and greater options. Leveraging mature and reliable communications and network technologies has allowed businesses to find the best-priced IT services virtually anywhere in the world. At the same time, outsourcers may be marketing directly to business units, diminishing the monopolistic service relationships fostered by some IT departments.

Although IT departments are losing some control as vendors and outsourcers sell directly to lines of business, IT professionals are emerging as essential resources for maintaining compliance. Regulations vary across national and sometimes state borders but depend upon a common framework of defining baseline standards, enforcing those standards, and implementing auditable change control procedures.

The final theme common to IT environments is budget constraints. The well-worn dictate “do more with less” is woven into the fabric of IT operations. When IT funding is increased, it is usually accompanied with additional responsibilities. One of the most cost-effective ways to deal with stagnant budgets and increasing demands is to cut maintenance costs. One researcher found that “Organizations that spend 76 percent on maintenance and are able to reduce maintenance by 10 percent realize a 7.6 percent savings. In contrast, a 10 percent reduction to their new development efforts (24 percent) yields just 2.4 percent.” (Source: Phil Murphy “APM Tools Will Reach \$500M To \$700M By 2008,” Forrester, 7/22/05.)

The combination of information-centric business drivers and the current state of IT creates an environment of constant or near-constant change. The need for change will continue for the foreseeable future, so IT managers must focus on controlling and managing that change.

Managing Change

Managing change is not about having a crystal ball that reveals the future but about understanding what is in place in an IT environment and being able to forecast possible changes and prioritize changes for existing and new components and services. Three essential aspects of effective change management include:

- Visibility and control
- Cost controls
- Impact analysis (financial and services)

Together, these factors enable effective and viable change management operations.

Need for Visibility and Control

Managers require visibility into some of the lowest-level details about an organization's infrastructure to effectively control the transition to new implementations. These details span the breadth of IT infrastructure to include:

- Server, desktop, and mobile device configurations
- Software and application packages
- Network configuration
- Event monitoring and tracking
- Security posture: vulnerabilities, threats, and breaches

Desktop configurations, for example, can vary widely even in organizations that standardize on platforms. For example, Windows XP may be a standard, but users of a third-party application may need to run Windows 2000. At the very least, IT will need to support two different OSs. If the third-party application is scheduled for an upgrade that supports Windows XP or if the application will be retired, the OS can be upgraded after one of those changes. Managing this dependency is yet another element of change control.

With frequent changes and updates to application packages and custom-built software, IT managers need the ability to track which versions or applications are deployed and where. Manually inventorying software is not practical; automated discovery is essential for efficiently managing software and applications packages. In addition to the speed at which automated discovery operates, automated discovery can provide precise details that would be time consuming to track manually.

Network services are another area where visibility into current configurations is necessary. As organizations grow and new services are introduced, networks become more complex. When businesses grow geographically, more networking hardware is required. Additional routers, firewalls, and switches are deployed. When new services are deployed, such as virtual private network (VPN) access for remote users or a Web interface to a back-office database, firewalls and security monitoring programs may require reconfiguration. It is essential for network administrators to understand the required changes and their impact on users in order to minimize any disruption in network availability.

Visibility is not limited to relatively static configurations. Systems and network administrators must have knowledge of the dynamic operations of their infrastructures:

- What events are occurring on the network?
- Are routing tables changing?
- Is there an unusually high volume of Simple Network Management Protocol (SNMP) messaging between devices?
- Did the notebook that just connected to the network download a required patch?

The combination of longer-term configuration information and event details provide a foundation for active change control.

Change management information also supports information security. Does a rapidly spreading virus or worm threaten your systems? The speed with which one can answer that question and deploy patches to mitigate the vulnerability can make the difference between preventing a security breach and responding with a costly and disruptive malware clean-up operation.

Visibility enables timely controls. Change management also requires cost-effective controls.

Maintaining Cost-Effective Controls

With large numbers of systems, a range of hardware platforms, and increasingly complex networks, the cost of maintaining change control systems can grow. Best practices gleaned from successful implementations can help to minimize those costs:

- Real-time or near real-time monitoring is necessary
- Support for incident and problem management is required
- Employee self-services are a necessity

Real-time monitoring enables technicians to respond to incidents before the effects of the incident spread and create unnecessary problems. With timely warnings, a malware-infected notebook can be quarantined and the malware removed before it infects other devices.

When disruptive incidents occur, such as the need to roll back a patch or install a security update, administrators need configuration and dependency information. The speed with which this information is retrieved is a determining factor in returning systems and applications to normal operating status.

As with any support operation, self-service applications can significantly reduce costs compared with delivering the same service through a call center.

Breadth of Change Management

Change management crosses organizational and technical boundaries. It is not the province of network management or application development or help desk support; it is the responsibility of all these departments. It also spans technologies and procedures to include hardware delivery, software installation and configuration, patch management, and related domains, such as information security and backup and recovery operations.

Case Study: Lafayette School Corporation

When the Lafayette School Corporation faced a 4,000 PC deployment, they turned to Altiris® Deployment Solution™. The benefits of that decision have extended to long after the hardware rollout. In addition to reducing the time to deploy new devices, the combination of Altiris® Helpdesk Solution™, Inventory Solution®, Software Delivery Solution™, and Carbon Copy® Solution has allowed the school district to shift systems management to a policy-based, time- and cost-efficient method.

With only eight technicians, 130 Dell servers, and 4,000 PCs at 19 facilities and two network centers, Lafayette School Corporation depends on proactive management and automated responses to keep up with maintenance tasks. For example, Inventory Solution can automatically start a defragmenting process when a PC's disk becomes 30 percent fragmented as well as initiate a work order with the help desk so that the help desk staff can respond before a critical situation occurs. As Kevin Little, director of Facilities and Technology Support, pointed out, "We need the proactive server protection Altiris software provides so that we don't have a failure that takes down hundreds of PCs."

Using Altiris applications not only improved the ability to provide system management services; it also allowed for radical changes in methods. For example, with 72 standard PC images for varying requirements, technicians are able to re-image a disk when troubleshooting will take longer than 30 minutes. Without this capability, support staff could easily spend days researching and solving system problems.

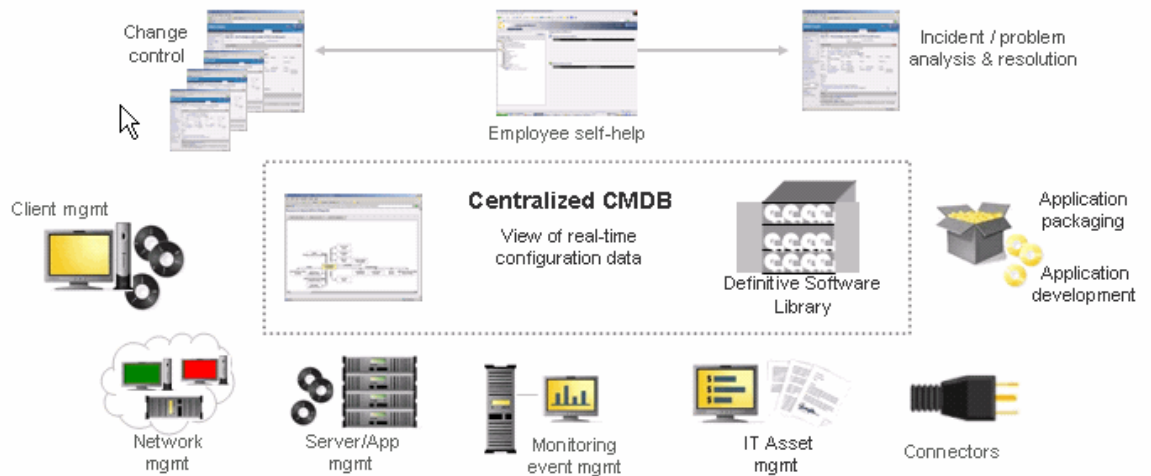
By effectively and efficiently providing system support with Altiris solutions, the Lafayette School Corporation can now channel resources that would have been allocated to IT operations to other business demands.

Effective Change Management Requirements

Effective change management is based on a combination of ready access to information and enforced policies and procedures. The first requirement is met with configuration management database (CMDB). This repository contains details of configuration items and relationships between them. Gartner defines the CMDB as including services to discover and integrate configuration information, federated data stores, visualization of infrastructure, and impact and risk analysis capabilities. Moreover, CMDB information is leveraged for change control, incident management, problem management, and security management (see Figure 1).

Figure 1

Configuration management database captures a broad range of infrastructure information and allows the alignment of Configuration Items (CIs) with delivered services.



By automating many of the time-consuming tasks in change management, such as gathering information and tracking dependencies, administrators and managers can focus on implementing and enforcing standard policies and procedures—monitoring and auditing procedures while analyzing trends and planning for future demands.

Summary

Information systems are subject to constant pressures to change. As businesses respond to market demands and conditions, IT managers must take action with appropriate technology implemented in a timely and cost-effective manner. At the same time, those same managers are expected to maintain and improve services and comply with growing bodies of regulations while under constant demand to control costs. Effective change-management procedures coupled with a centralized CMDB has proven an effective method for stabilizing the management of dynamic and complex information systems.