realtimepublishers.com®

The Definitive Guide™ To

Service-Oriented Systems Management

Dan Sullivan

Introduction to Realtimepublishers

by Don Jones, Series Editor

For several years, now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: The State of Systems Management

The information technology (IT) in an organization is a dynamic resource that is constantly adapted to meet changing needs. The rational practice of controlling that change is known as systems management. As with many other organizational practices, systems management has evolved from informal ad hoc responses to immediate needs to a well-understood, formalized practice. This guide examines best practices for systems management with an emphasis on a modularized approach known as service-oriented management (SOM).

Overview

The book consists of twelve chapters that begin with a background on systems management practices, then describes SOM in terms of several well-known frameworks for systems management and related areas, and finally moves on to a detailed discussion of how to implement SOM. Specifically, the chapters will address:

- Chapter 1 discusses the goals of systems management, typical implementation styles, and the need for a rationalized process, such as SOM.
- Chapter 2 describes essential parts of systems management, including aligning with business objectives, managing assets, delivering services, and maintaining compliance.
- Chapter 3 discusses SOM in terms of well-known frameworks such as ITIL, COBIT, and ISO-17799.
- Chapter 4 describes the infrastructure required to implement a rational, efficient systems management environment, including a configuration management database.
- Chapter 5 examines the elements of service support, such as incident, configuration, and change management.
- Chapter 6 explores how to address financial issues, capacity planning, and availability management issues in SOM.
- Chapter 7 discusses application life cycles, software asset management, and managing hardware elements of IT infrastructure.
- Chapter 8 looks at systems management as a tool for supporting control objectives and management guidelines that govern IT operations.
- Chapter 9 examines the role of systems management in threat assessments, vulnerability management, incident response, and other aspects of security management.
- Chapter 10 describes the practice of risk management and shows how identifying risks, prioritizing assets, and mitigating risks serve both risk management and systems management objectives.
- Chapter 11 examines the business case for SOM with particular attention paid to the cost of not adequately managing systems.
- Chapter 12 describes how to assess the current state of an organization’s systems management practice and how to plan the transition of a SOM model as well as provides guidance on how to implement a mature systems management practice.

The responsibilities of systems administrators and IT managers are growing in complexity. The need to support a growing number of systems with increasing dependencies between those systems, meet growing quality of service (QoS) expectations, and be prepared for constant security threats are just a few of the challenges faced by systems managers. Fortunately, as the demands have expanded so too have the tools and practices for meeting those demands. The purpose of this guide is to help managers and administrators apply these practices and tools to their specific systems management challenges.

This chapter presents a high-level overview of the nature of systems management with a discussion of three aspects of the discipline:

- The goals of systems management
- The spectrum of systems management practices
- Rationalizing systems management with SOM

Let’s begin with a fundamental issue for all IT operations—aligning with business objectives.

Goals of Systems Management

Systems management serves many purposes. To a systems administrator, systems management is about keeping servers up and running, keeping databases responsive to user queries, and ensuring the network continues to function. To IT managers, systems management is the means to another set of ends, including meeting service level agreements (SLAs), controlling operations costs, and meeting production schedules. To executives, systems management is an area for controlling the integrity of information and maintaining compliance with any number of regulations that may apply to the business.

There is quite a bit of overlap between the different perspectives on systems management, and the key purposes include four fundamental objectives:

- Business alignment
- Technical integrity
- System availability
- Compliance

These objectives provide the measures and criteria to which the systems are maintained and controlled. These are the goals of systems management.

Business Alignment

The objective of business alignment is to ensure that the information processing needs of lines of business (LOB) are met by IT applications and infrastructures. This sounds so logical that it seems like common sense—and it is. Unfortunately, the constraints of real-world organizations present significant challenges to realizing business alignment.

The challenge with business alignment is not in understanding the need for it or even convincing business or IT personnel about its importance; the challenge is with the execution. Three common problems encountered with business strategy execution are:

- Formulating a coherent business strategy
- Addressing multiple objectives
- Meeting dynamic requirements

In many cases, IT managers have to address one or more of these in the course of their systems management work.

Coherent Business Strategy

The first challenge is articulating a coherent business strategy. Again, what seems simple at first glance is actually quite involved. Businesses have the general goal of maximizing revenue. They do so by implementing strategies related to product development, acquiring market share, forming partnerships, and so on. Large and even midsized organizations constantly run into the problem of multiple perspectives on a single strategy.

Consider an example of an insurance company selling auto insurance. The company’s strategy may include building market share in the northeast and mid-Atlantic regions of the United States. Marketers in corporate headquarters might want to initiate a set of campaigns to build market share that may conflict with the objectives of executives responsible for third-party brokers in that region. Similarly, the Underwriting department may want to exclude a certain demographic group, such as male drivers under 32, even though that is one of the demographic groups that Marketing would like to target. Add to these issues the fact that the business case for a particular strategy is based on revenue projections that include measures such as profit margins that are calculated differently by different LOB. Before IT operations can align with business strategy, the strategy must be well defined.

Multiple Business Objectives

A second difficulty with business alignment is meeting complementary needs with a minimum number of applications. Continuing with the insurance example, both internal sales staff and third-party agents may need to use the same policy origination system to sell insurance. Internal sales staff may use direct mail and telemarketing as the primary means to generate sales. They work in company offices and prefer a client/server model for the policy origination system. Third-party agents, however, sell products from multiple insurers and have no interest in having a client application installed on their computers from each of their partners. Web-based applications are preferable to them because applications can be downloaded on demand, do not require permanent installations, and entail fewer maintenance issues for users. Application developers are now faced with either maintaining two interfaces, one client/server and one Web, or trying to implement full client/server functionality in a Web application. The application interface is just one example of juggling multiple requirements.

In addition to the transaction-oriented operations that involve large numbers of relatively simple read-and-write operations, such as creating policies and submitting claims, users need management reporting to understand the overall state of business. Claims adjusters may want to understand trends in claims by policy type, by characteristics of the policy holder, and by geographic region. This type of aggregate reporting is common but functions best under a different set of database design models than transaction-oriented systems. Management reporting, or business intelligence reporting, works best when done with operational data stores for short-term integrated reporting and data marts and data warehouses for historical reporting and trend analysis. Here again, IT is left to create, maintain, and manage another set of systems.

Dynamic Requirements

Business must constantly respond to changes in the marketplace. Some of these changes are relatively slow, such as the move from strictly internal combustion powered cars to hybrid cars, some are more moderately paced, like the shift to buying downloadable music from buying it on discs, and still others are rapid changes, such as price spikes in the cost of petroleum products. How effectively an organization can respond to these changes is dictated, in part, by the organization's ability to change its IT systems. Consider some of the roles IT applications play in adapting to market changes:

- As partnerships are formed with other business, financial systems must be changed to accommodate new compensation models
- Following mergers, IT infrastructures must be integrated to accommodate combined business operations
- Downward price pressures drive process re-engineering and the adoption of greater automation
- Outsourcing of operations may require changes to network infrastructure, security policies and practices, and hardware configurations

In addition to these common business dynamics, there are the expected but unpredictable events, such as natural disasters, that can disrupt operations and shift priorities.

There will always be a time delay between changing a business objective and making the necessary changes to implement that in IT infrastructure and procedures. The length of the delay, though, can have a qualitative impact on the ability to execute the new business operations. As Figure 1.1 shows, IT responses may take so long that not long after they are implemented, new changes are required. In the worst case, the modifications are not finished before the next round of changes is defined.

Aligning IT operations with long-term business strategies and shorter-term objectives is a process; it is not a static state that is ever reached. The goal of IT should be to minimize the time it takes to align with business objectives, and well-developed systems management practices are fundamental to reaching that goal.

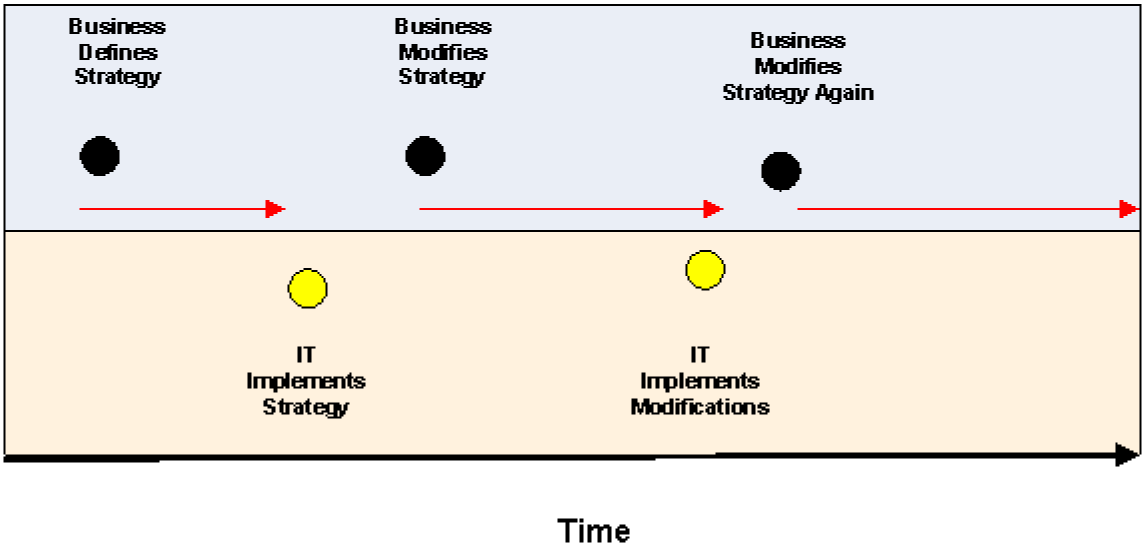

Business Defines Strategy
Business Modifies Strategy
Business Modifies Strategy Again
IT Implements Strategy
IT Implements Modifications
Time

Figure 1.1: Time delays between the change of business strategy and the ability of IT to implement slow the ability of organizations to adapt to changing market conditions.

IT and business alignment is based on a number of assumptions, including the technical integrity of the IT infrastructure.

Technical Integrity

Technical integrity is the quality of information systems that ensures data is accurate, reliable, and not subject to malicious or accidental changes. Like business alignment, technical integrity is one of the characteristics that are so logical that we take it for granted. Systems administrators do not take it for granted, though. Consider some of the challenges to maintaining technical integrity:

- Malfunctioning applications
- Malicious software
- System configuration vulnerabilities
- Improperly managed access controls

Each of these categories of threats can create substantial disruption to IT operations.

Malfunctioning Applications

Let's face it, software has bugs. Complex software is difficult to build and programmers know this all too well; an old quip among programmers is that "if builders built buildings the way programmers built programs, one woodpecker would destroy civilization." Although this statement is an obvious exaggeration, the sentiment reflects the frustration even software developers have with the practice of programming.

> Programmers and software engineers do not just decry the state of programming; much work has been done to improve software development practices. See for example, software development maturity models developed by the Software Engineering Institute at http://www.sei.cmu.edu/, spiral development methodology at http://ieeexplore.ieee.org/iel1/2/6/00000059.pdf?tp=&arnumber=59&isnumber=6&htry=2, and Agile development methodology at http://zsiie.icis.pcz.pl/ksiazki/Agile%20Software%20Development.pdf.

Using software development best practices can increase the quality of software, but even with these methodologies, the impact of tracking and eliminating all bugs would make any reasonably complex program either too expensive or available too late to be of practical use. As a result, users, systems managers, and developers have all learned to manage less-than-perfect applications.

One practice used to manage software deficiencies is patch management. Software developers release corrections to applications, known as patches, which are applied by systems administrators or through an automated process to correct known errors in software. Patching is not a trivial process and several factors should be considered when patching:

- How to implement user acceptability testing (UAT)
- How to roll back a patch if problems occur
- Whether any of the problems corrected by the patch will have an impact on operations
- How to distribute the patch to all systems that require it
- How to track the version and patch level of all applications

In addition to these basic considerations, applications may have issues. For example, a relational database may be used to support two applications. One application does not function because of a bug that can be patched but the patch breaks another function required by the second application. Should the database administrator patch the system anyway? Keep the current version and work around the bug? Install another instance of the database, patch one instance, leave the other instance un-patched, then run the two applications on their respective instances of the database? To find the right answer, systems administrators and database administrators have to weigh the costs and benefits. Just as business objectives can create competing demands when addressing IT and business alignment, patch management can leave systems administrators to choose between equally undesirable options.

Malicious Software

Malicious software, commonly known as malware, includes software that ranges from annoying to destructive. Some of the best known forms are:

- Viruses—Programs that replicate with the use of other programs or by user interaction and carry code that performs malicious actions. Viruses consist of at least replication code and the payload but may also include encryption of code-morphing routines to improve chances of avoiding detection.
- Worms—Similar to viruses in payload and obfuscation techniques, worms are self-replicating.
- Spyware—Software that installs on devices without user consent and collects private information, such as usernames, passwords, and Web sites visited.
- Trojan horses—Programs that purport to do one thing but perform malicious activities. For example, a Trojan horse might advertise itself as a program for synchronizing computer clocks to atomic clocks, but it may deploy a remote control program that listens on a specific chat room or Internet Relay Chat (IRC) channel for commands from the malware developer.
- Keyloggers—Programs that intercept operating system (OS) messages sending keystroke data to applications. The more sophisticated versions of these programs filter most activity to focus on usernames, passwords, and other identifying information.
- Frame grabbers—Software that copies the contents of video buffers, which store data about the contents displayed on the computer's screen.

The list of malicious software categories is intimidating. To make matters worse, malware writers seem to be in a constant cycle of responding to anti-malware developer's countermeasures who then respond to the malware writer's new tricks, and on and on. On the positive side, systems administrators are able to keep malware at bay with effective anti-malware devices.

The use of anti-malware software, such as desktop antivirus software, and network appliances, such as content filters, can provide adequate protection for most needs. The need for these countermeasures introduces additional responsibilities for systems administrators. In addition to the desktop productivity applications, application servers, databases, routers, Web servers, and all the other business-specific and supporting tools that must be managed in an IT environment, systems administrators must now manage a large class of mission-critical security applications and devices. Malicious software often takes advantage of poorly secured configurations.

System Configuration Vulnerabilities

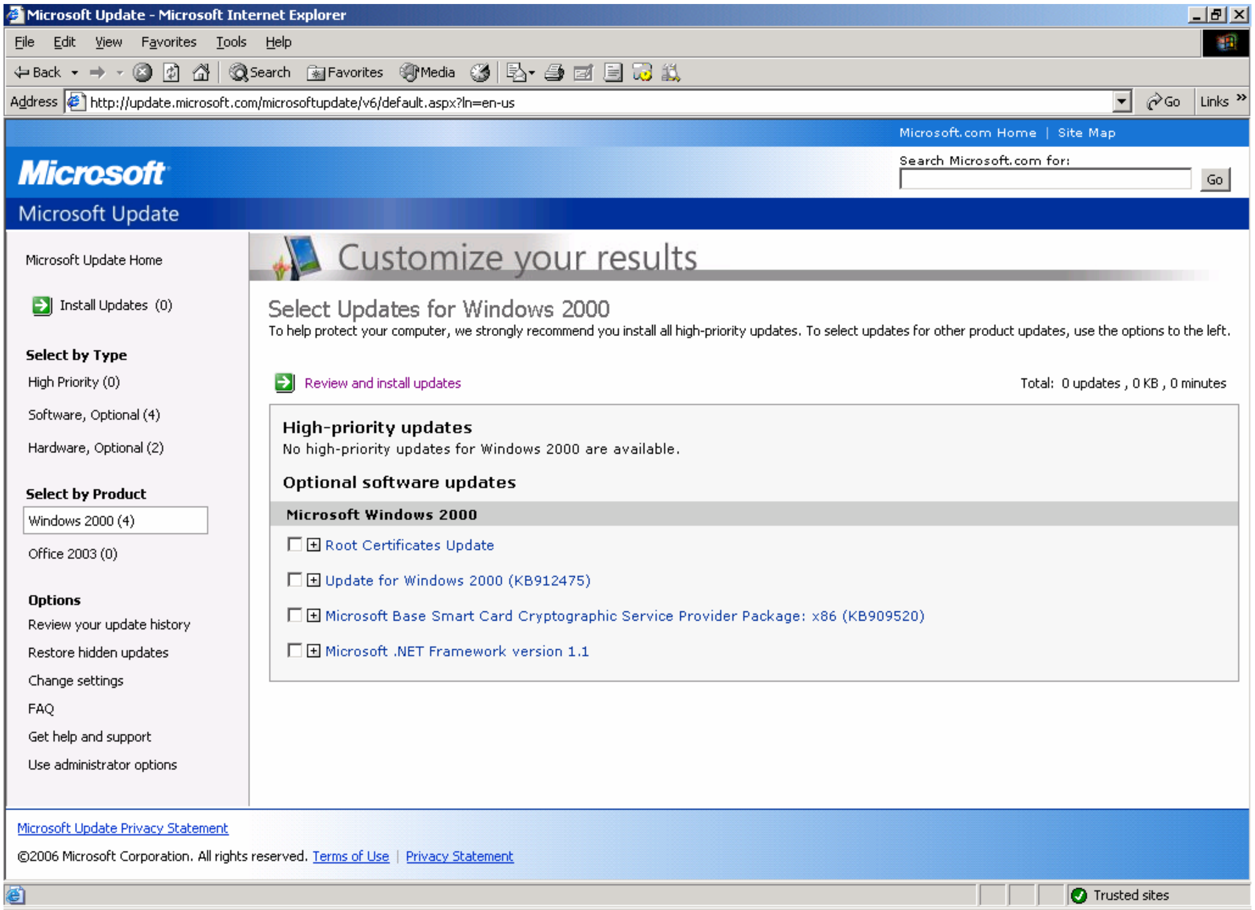
Another threat to system integrity is configuration vulnerabilities. It has been a common practice to ship complex software with standard configuration that works “out of the box” on most systems. The goal is to make software as easy to install and use as possible. This goal is understandable; we do not expect to have to master the intricacies of a new application just to install it. The problem with this approach is that to make software functional with minimal user intervention on a wide variety of machines, applications tend to install services that are not always needed, highly privileged accounts, or other potential security vulnerabilities:

- A mini-computer OS commonly used in the 1980s and 1990s installed with three privileged accounts with commonly known passwords.
- Some older database systems install with well-known privileged accounts with known passwords.
- Selecting predefined OS configurations, such as a server configuration, can install programs services, such as ftp, that may not be needed and may introduce security vulnerabilities.

Software vendors are getting better about installing more secure default configurations, but as systems grow in complexity, the potential for insecure configurations grows as well.

Another aspect of configuration vulnerabilities is that installed systems may require patching. Such is especially the case when an OS is first installed; security patches created since the software was released should be installed immediately. This task can be relatively easily and automated or it may require significant effort on the part of systems administrator.

Microsoft, for example, provides the Microsoft Update service for Windows OSs, which can be configured to automatically download and install critical patches (see Figure 1.2).



http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us

Customize your results

Select Updates for Windows 2000

To help protect your computer, we strongly recommend you install all high-priority updates. To select updates for other product updates, use the options to the left.

Review and install updates

Total: 0 updates , 0 KB , 0 minutes

High-priority updates

No high-priority updates for Windows 2000 are available.

Optional software updates

Microsoft Windows 2000

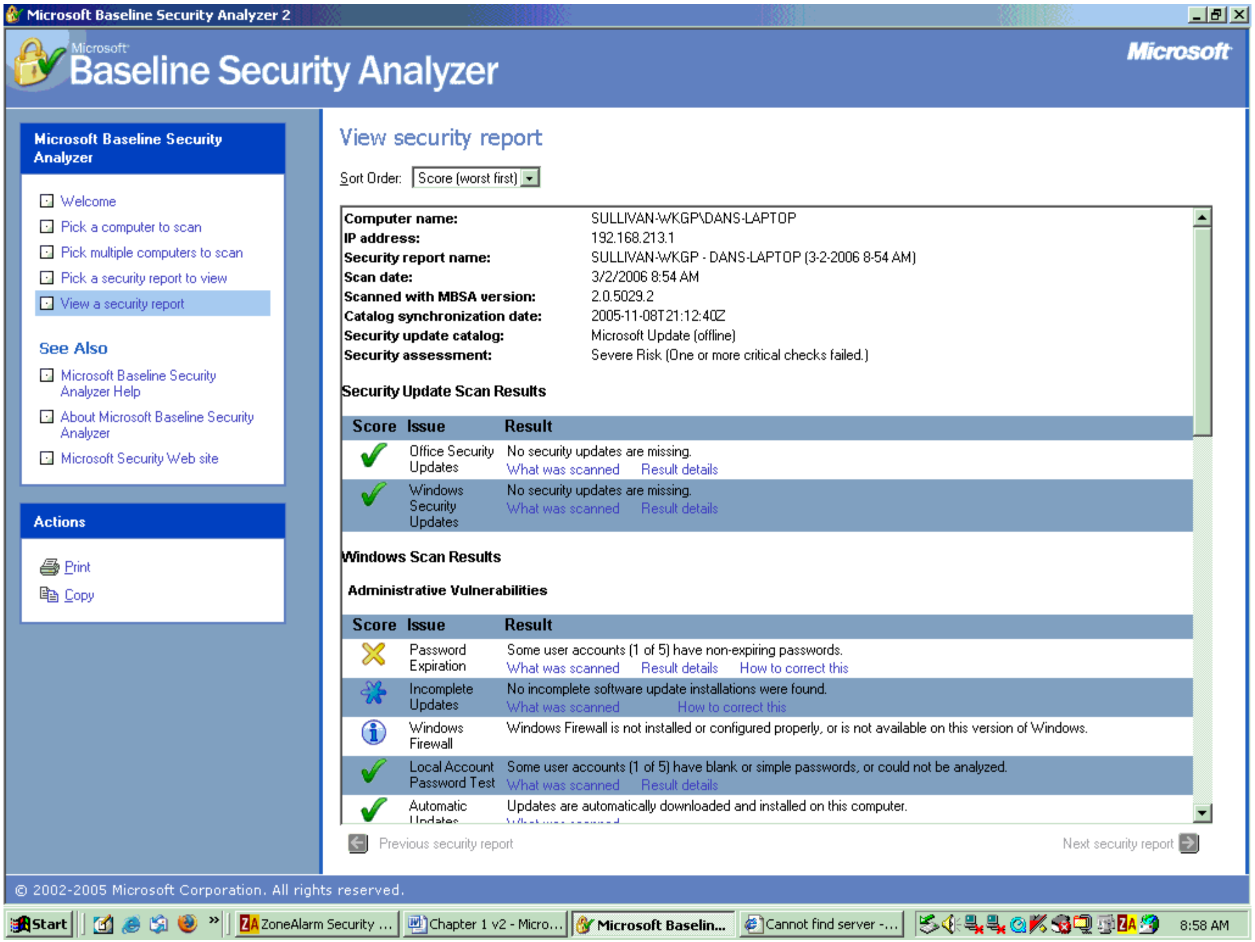
- □ ⊞ Root Certificates Update
- □ ⊞ Update for Windows 2000 (KB912475)
- □ ⊞ Microsoft Base Smart Card Cryptographic Service Provider Package: x86 (KB909520)
- □ ⊞ Microsoft .NET Framework version 1.1

Microsoft Update Privacy Statement

©2006 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement

Figure 1.2: The Microsoft Update service can determine necessary critical patches and install them on Windows OSs.

For more thorough vulnerability scanning, the Microsoft Baseline Security Analyzer (MBSA) can detect configuration vulnerabilities as well as missing patches, and MBSA allows systems administrators to scan multiple systems in a single session.


Microsoft Baseline Security Analyzer 2
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
□ Welcome
□ Pick a computer to scan
□ Pick multiple computers to scan
□ Pick a security report to view
□ View a security report
See Also
□ Microsoft Baseline Security Analyzer Help
□ About Microsoft Baseline Security Analyzer
□ Microsoft Security Web site
Actions
Print
Copy
Previous security report
Next security report
© 2002-2005 Microsoft Corporation. All rights reserved.
Start
ZoneAlarm Security ...
Chapter 1 v2 - Micro...
Microsoft Baselin...
Cannot find server -...
8:58 AM

View security report

Sort Order: Score (worst first)

Computer name:	SULLIVAN-WKGP\DANS-LAPTOP
IP address:	192.168.213.1
Security report name:	SULLIVAN-WKGP - DANS-LAPTOP (3-2-2006 8-54 AM)
Scan date:	3/2/2006 8:54 AM
Scanned with MBSA version:	2.0.5029.2
Catalog synchronization date:	2005-11-08T21:12:40Z
Security update catalog:	Microsoft Update (offline)
Security assessment:	Severe Risk (One or more critical checks failed.)

Security Update Scan Results

Score	Issue	Result
✓	Office Security Updates	No security updates are missing. What was scanned Result details
✓	Windows Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Password Expiration	Some user accounts (1 of 5) have non-expiring passwords. What was scanned Result details How to correct this
✱	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
ⓘ	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
✓	Local Account Password Test	Some user accounts (1 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned

Figure 1.3: The Microsoft Baseline Security Analyzer scans systems for vulnerabilities as well as missing patches.

In other cases, systems administrators must keep abreast of critical patches by subscribing to mailing lists or checking vendors' support Web sites to finds patches. Even when patches are released, they should not be installed in production without first testing on a quality control platform. Although installing a critical security patch for Windows can create unanticipated problems, in most cases, the risks are far outweighed by the benefits. Nonetheless, systems administrators should have a contingency plan in place for restoring the original configuration if unanticipated problems occur.

> Two useful security-oriented mailing lists are NTBugtraq (http://www.ntbugtraq.com/) and Secunia (http://secunia.com/).

💣 It should be noted that even with security analyzing tools, one type of malware—rootkits—are particularly difficult to control once they have compromised a system. Rootkits hide their presence and activities by changing registry settings or other system parameters, hiding files, erasing log entries, and other techniques. Once installed, it is difficult to guarantee that rootkits have been removed without performing a full reinstall of system software.

Even with updated patches, securely configured servers and desktops, and malware countermeasures, systems managers must contend with yet another threat: inappropriate access controls.

Improperly Managed Access Controls

Access controls grant privileges to employ information resources to users typically based on users' role in the organization. A CFO is likely to have full read access to any data in the financial system while an accounts payable clerk would have no access or highly restricted access to accounts receivable information. This variance in access based on roles reflects one of the goals of security administrators, which is to ensure that users and processes have the least privilege required to accomplish their functions. Although the CFO and accounts payable clerk examples are relatively simple, determining least privilege can become more complex. For example

- What rights to an inventory system should a third-party partner have? Should he or she be able to reserve inventory or just check the status of products?
- Should a manager in the southwest region have data warehouse reports on the northeast region?
- When an average user searching an enterprise portals for "salary" see a listing for a file called Current_Salary.xls even though the file can only be read by HR personnel?
- If a network administrator is terminated, how can management be sure all of his rights to systems are revoked?

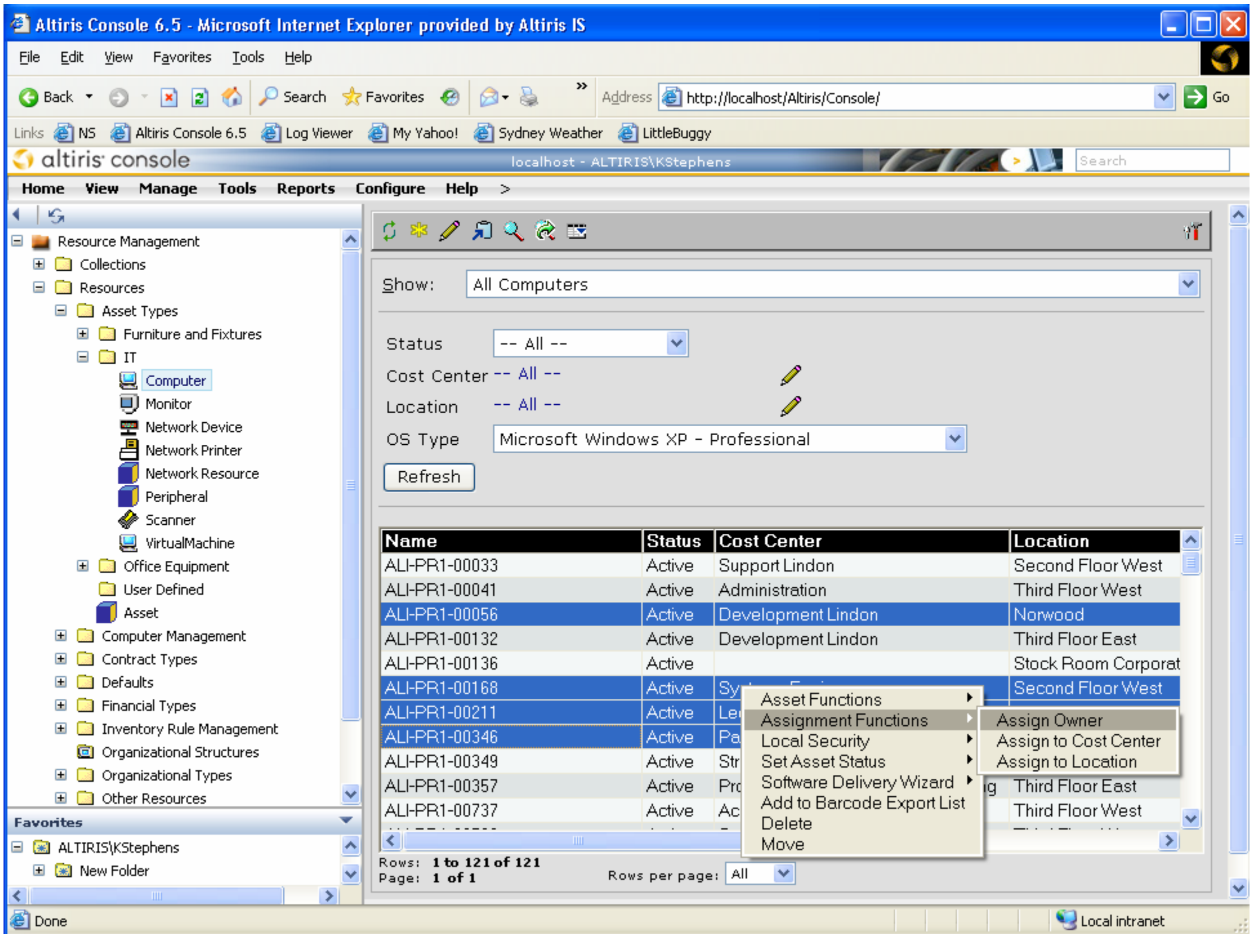
Managing access controls is a complicated and, in some cases, time-consuming process. One of the objectives of systems management is to ensure that access controls are synchronized with organizational policies at all times. These policies should include descriptions of who is allowed administrator access to systems, password strength and term of use, and audit procedures.

Maintaining the technical integrity of multiple servers, desktops, mobile devices, and network components requires a thorough understanding of application and OS configurations, countermeasures to threats from malicious software, and effective access controls and other security measures. Closely related to the issue of technical integrity is systems availability.

System Availability

Disasters happen. Some are natural, such as hurricanes, and some are technical, such as the SQL Slammer worm that effectively shut down large segments of the Internet in 2003. In both cases, businesses and organizations lose some degree of access to their systems. The practice of business continuity planning has evolved to address these kinds of disasters as well as other less dramatic events that can nonetheless have an impact on systems availability.

Systems administrators play a key role in continuity planning because of their knowledge of systems organizations, dependencies between systems, and the process that operate on those systems. As IT infrastructure becomes more complex, business continuity planning become more difficult. Information about the state of IT systems is needed to adequately prioritize services (for example, in the event of a service disruption, restore payroll systems and then customer service systems, leaving other production system for later) and ensure that all necessary systems and processes are accounted for. A centralized and up-to-date database with information on the IT infrastructure is required for cost-effective business continuity planning and execution. Figure 1.4 shows an example of how IT assets can be centrally managed in relation to other assets and organizational structure.



Show: All Computers

Status -- All --

Cost Center -- All --

Location -- All --

OS Type Microsoft Windows XP - Professional

Name	Status	Cost Center	Location
ALI-PR1-00033	Active	Support Lindon	Second Floor West
ALI-PR1-00041	Active	Administration	Third Floor West
ALI-PR1-00056	Active	Development Lindon	Norwood
ALI-PR1-00132	Active	Development Lindon	Third Floor East
ALI-PR1-00136	Active		Stock Room Corporat
ALI-PR1-00168	Active	Sy	Second Floor West
ALI-PR1-00211	Active	Le	
ALI-PR1-00346	Active	Pa	
ALI-PR1-00349	Active	Str	
ALI-PR1-00357	Active	Pr	Third Floor East
ALI-PR1-00737	Active	Ac	Third Floor West

Rows: 1 to 121 of 121
Page: 1 of 1
Rows per page: All

Figure 1.4: Centralized information about IT assets is a key enabler of effective business continuity planning.

📖 For more information about the structure and function of configuration management databases, see Chapter 4.

Compliance

The term *compliance* is getting a lot of press these days, perhaps to the point where we've stopped paying attention to it, but doing so would be a mistake. The importance of maintaining the privacy and accuracy of information is becoming more broadly recognized. Some of the best known regulations make that clear:

- The Health Insurance Portability and Accountability Act (HIPAA) defines categories of "protected healthcare information" and strict rules governing how that information is gathered, stored, used, and shared. The act also defines stiff penalties for violating these rules.
- The Sarbanes-Oxley Act, enacted in the wake of Enron, WorldCom, and similar corporate scandals, raises the bar on ensuring accuracy in corporate reporting. CEOs and CFOs now have to sign off on the accuracy of the information or face penalties.
- The California law, State Bill 1386, was passed in response to fears of the growing threat of identity theft. Under this law, if identifying information of a California resident is stolen or released in an unauthorized manner, the resident must be notified of the disclosure.

A host of other IT-related regulations have been enacted by governments around the world. In addition, non-governmental or quasi-governmental bodies have adopted standards and frameworks related to financial reporting and security best practices. Table 1.1 lists some relevant but less well-known regulations and frameworks that apply to particular countries or industries.

Regulation/Framework	Description	For More Information
BASEL II	Regulates credit and risk reporting for banks	http://www.bis.org/publ/bcbsca.htm
21 CFR Part 11	Regulates pharmaceutical information management	http://www.fda.gov/ora/compliance_ref/part11/
Computer Fraud and Abuse Act	Makes unauthorized access to information in federal and financial institutions illegal	http://cio.doe.gov/Documents/CFA.HTM
Electronic Signatures in Global and National Commerce Act	Recognizes the use of electronic signatures in commerce	http://www.ecloz.com/ecloz/Electronic%20Signatures%20in%20Global%20&%20National%20Commerce%20Act-%20H_R_%201714.htm
FFEIC Business Continuity Planning	Regulates business continuity planning in financial institutions	http://www.ffiec.gov/ffiecinfobase/html_pages/bcp_book_frame.htm
Gramm-Leach-Bliley Act	Regulates consumer privacy in banking	http://banking.senate.gov/conf/grmleach.htm
FISMA	Regulates information security planning in federal agencies	http://csrc.nist.gov/sec-cert/index.html
EU Directive 95/46/ EC - Data Protection and EU Directive 2002/58 EC – Directive on Privacy	Controls the use and distribution of personal information of EU citizens	http://europa.eu.int/comm/internal_market/privacy/law_en.htm and http://europa.eu.int/eurlex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
Canada's PIPEDA	Protects personal information of Canadian citizens	http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp.
Australian Federal Privacy Act	Enacts Australian privacy principals	http://www.privacy.gov.au/publications/npps01.html

Table 1.1: Additional regulations related to IT.

These and similar regulations are placing new demands on IT mangers and systems administrators to not only comply with these regulations but also demonstrate that they are in compliance. As with business continuity planning, compliance requires a centralized management view of all information assets to meet these demands efficiently.

The goals of systems management range from maintaining technical integrity and system availability to achieving compliance with regulations and aligning with the strategic plans of the business. These are demanding goals and reaching them is not guaranteed, especially if systems management practices are not sufficient for the task.

Spectrum of Systems Management Practices

Systems management, like other areas of IT management, has a range of management philosophies. Some are loosely coupled procedures that are created—and evolve—as needed in response to immediate needs, while others are highly structured and formalized around written policies. For the purposes of this guide, it helps to examine three high-level categories of systems management practices:

- Ad hoc systems management
- Controlled systems management
- Continuously improving systems management

This list is not meant to be exhaustive and there are nuances within each category that will not be examined. The goal is to understand that not all systems management practices are the same—some are more viable than others—and that the level of effort required of and effectiveness realized from different practices can vary widely.

Ad Hoc Systems Management

At one end of the systems management spectrum is the ad hoc style, which is characterized by a lack of formal policies and procedures. This approach to systems management responds to requirements, incidents and problems as they arise without the benefit of planned responses. The results are suboptimal, at best.

Ad Hoc Systems Management in "Practice"

Consider scenarios that can arise when ad hoc systems management is used:

- A user needs a utility for managing ftp transfers, so he downloads several evaluation versions from the Web. After some time, he decides to purchase one while a colleague, with a similar problem, decides she likes a different program. Both purchase the programs outside their departmental budgets with no review or approval from IT. When problems arise with the programs, the users call the IT department, which is unaware the programs are used in the organization.
- Policies are not in place governing email use. Old messages are not automatically archived, content is not filtered for inappropriate material, and rules are not defined regarding appropriate use of company email. As email servers run out of disk storage, more is purchased; all message folders are backed up and backups are taking longer and longer to run. Email server software is patched when a systems administrator reads about a new threat in weekly trade magazines.
- Users dictate means of collaboration, which typically involves sharing local folders and creating common use folders on the network server. Folders are shared when a user needs to share files and folder, and owners can change directory permissions at will. There is no centralized repository of information about who has access to which directories. Employees that left the company several months ago still have permissions to sensitive directories and files.

- A department decides that the reporting from the financial system is insufficient for their needs and installs a database and reporting tool on a high-end desktop computer running in their office. One of the staff in the department just read a book on data marts and decides to implement one. The department uses an extraction, transformation, and load tool that came with the database to pull data from the financial system every night. This task puts additional load on the financial system at the same time it runs close-of-day batch jobs and delays the generation of morning financial reports. The reports generated from the data mart use different calculations, so performance measures from the financial system do not agree with those from the data mart.

Although these examples are fictitious, the consequences described will probably sound familiar to many IT professionals. A lack of central planning, uncoordinated decision making, and the willingness to make changes to IT infrastructure to meet an immediate need without concern for the ripple effects on the rest of the organization are the hallmarks of ad hoc systems management practices. The consequences are predictable.

Effects of Ad Hoc Systems Management

The lure of ad hoc systems management is that it appears responsive and unencumbered by unnecessary bureaucracy. If a user needs a program, he gets one. When an analyst needs better reporting, she develops her own Microsoft Access database. If the server runs low on space, the administrator buys another disk. Decisions are made quickly and executed just as rapidly. The consequences from these decisions, like the effects of a degenerative disease, accumulate over time.

Poor Management Reporting

One of the first noticeable impacts of ad hoc management is a lack of overall understanding of the state of the IT infrastructure. There is no place a manager can go to find a list of assets, their patch levels, the licenses associated with them, the state of their backups, or the applications running on particular devices.

Lack of Compliance

Auditors would quickly point out that a lack of well-defined policies and procedures leave the company potentially in violation of regulations governing information integrity (for example, the Sarbanes-Oxley Act) and privacy (such as HIPAA).

Inefficient Allocation of Resources

Poor management increases costs as well. Rather than manage storage, some would rather “throw another disk” at the problem, adding the immediate cost of new hardware and the ongoing cost of supporting the additional hardware to IT spending. When infrastructure grows, known as “server sprawl,” without an overall plan, there is the potential for a new hardware configuration that requires a new software configuration, which just adds to the management headaches of administrators. And because an organization is dealing with an ad hoc management attitude, tools such as a configuration management database are not available to shoulder the burden of additional configurations. Other costs creep in because of poor use of resources. For example, instead of sharing a disk array among multiple departments, each department may buy their own direct connect storage with each server, along with backup devices for each department. Without centralized planning, there is little opportunity to leverage the economies of scale.

Poor Security

Security suffers because of poor management practices. Malicious software, information theft, and other threats are a constant problem for systems administrators and IT managers. At the very least, basic information security management requires:

- Comprehensive inventory of hardware and software in use on a network
- Configuration details on all servers, desktop, mobile devices, and network hardware
- Detailed information on users and access controls protecting assets
- The ability to audit and monitor system and network activity and to identify anomalous events
- The ability to deploy patches and critical updates rapidly to all vulnerable devices

Clearly, the lack of centralized management information and ineffectual or poorly implemented procedures that characterize ad hoc management undermine even the most basic security requirements.

Lack of management controls, poor use of resources, lack of compliance, and the potential of security threats should be motivation enough to move beyond ad hoc management to a well-defined and centrally controlled management model.

Controlled Systems Management

As IT organizations grow and mature, the need for planning and control becomes more pressing. The disadvantages of ad hoc management are apparent; the advantages of well-defined policies and procedures are equally obvious. Industry best practices for systems management have been defined in two frameworks: the IT Information Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT).

> 🕮 For more information about ISACA's COBIT, see http://www.isaca.org/cobit/, and ITIL at http://www.itil.co.uk/. These topics are also covered in more detail in Chapter 3.

In a controlled systems management environment, the core IT operations are performed according to a series of policies that attempt to realize broad business goals by providing reliable and responsive computing and network resources at the most efficient cost. The core processes within IT that should be governed by policies are:

- Acquiring infrastructure, such as hardware, software, and networking services
- Developing, customizing, and configuring applications
- Implementing security controls
- Managing service providers
- Monitoring performance and capacity planning
- Ensuring system availability
- Managing end user support
- Training, both IT and non-IT staff
- Maintaining regulatory compliance

The policies addressing each of these areas define the purpose of the operation, identify the scope of the process, and offer guidelines for implementing the policy. For example, the purpose of implementing security controls is to ensure the integrity, confidentiality, and availability of information services. The scope includes areas such as physical security, access controls, telecommunications, and network security, as well as auditing and system monitoring. The guidelines surrounding security might include a discussion of the need to balance security with ease of use and the risk level acceptable to the organization.

Procedures are a series of specific tasks that implement a policy. For example, the procedure for acquiring software might include a review of the business requirements and deficiencies in existing software and an assessment of buying instead of building a solution. Next, the procedure might call for a review of the proposed solution. Which OSs does the application run on? What kind of server is required? What changes to the network configuration are required? Will the application be accessible from beyond the firewalls? Does it depend on other services, such as a Web server, on the network? After these steps are performed, the final stage may be a review by a change control committee made up of application owners, network administrators, and systems managers who make one last review for potential problems with the solution.

To some, these steps may sound like bureaucratic overkill, but it is better than the alternative presented by ad hoc management. Controlled systems management builds on policies and procedures that recognize that IT operations consist of a series of services, such as client management, network management, application management, and so on—not just a collection of independent, unrelated devices and programs as understood within the context of ad hoc management (see Figure 1.5).

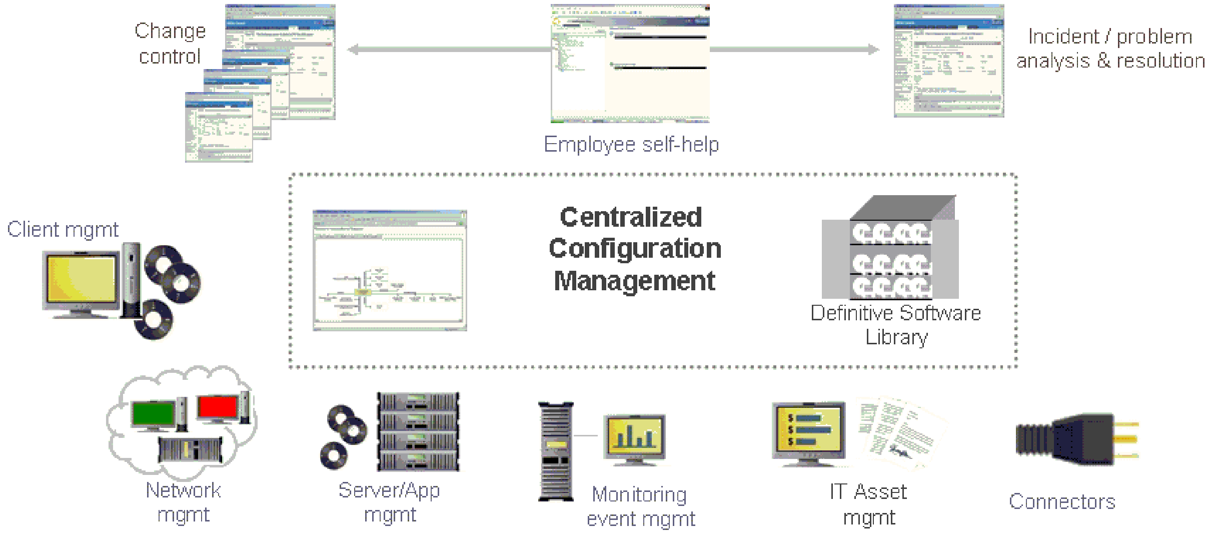


Figure 1.5: Controlled systems management depends on well-defined policies and procedures that address each of the key services provided in an IT environment.

It is not the goal of controlled management to slow IT operations or impose arbitrary bureaucratic overhead. In fact, controlled management improves responsiveness and effectiveness in the *long run* even though it may seem to slow changes or acquisitions in the short term.

There are two ways to streamline controlled management, and they dovetail well. First, centralize management information and automate routine tasks. A centralized configuration management system is the foundation for this method and will be discussed in detail in Chapter 4. The second is to leverage the information in the centralized configuration management system (along with data about how procedures are implemented) to improve the way you implement the tasks of systems management.

Continuous Improvement

Much has been written in the popular business press about quality and improvement. These topics do not garner the press they once did, but the principals of quality improvement and innovation are still relevant, even in systems management. Perhaps the best-known and most well-established approach to realizing continuous improvement is Six Sigma, a data-centric quality approach; another practice, Management by Fact (MBF), also emphasizes the importance of managing by using measurements of performance.

Once an IT group has implemented controlled systems management practices, the group will have information about assets, business use of those assets, and the changes those assets undergo. In essence, the organization will have procedures for effectively managing assets as well as data about the performance of those assets and related operation. With this, IT managers and systems administrators can find ways to improve on operations.

For example, by measuring the time from identifying the need for a new application to deploying the solution, as well as key milestones in between, the organization can better understand the average time to deploy, common bottlenecks in the process, and shared characteristics of failed efforts. These and other key performance indicators (KPIs) form the foundation for measuring improvement.

Another example relates to security. If a security breach occurs, a well-managed environment will have audit trails and logs to help diagnose the breach as well as recovery procedures for getting operations back online and data restored to its correct state. Configuration management information, along with audit trails and logs, can help identify both specific and general vulnerabilities in the current environment, which can be addressed to prevent future breaches of the same sort.

Exceptionally well-run IT operations are not the result of one or two geniuses formulating a perfect solution; they are instead the product of disciplined policies and procedures tightly linked to business objectives. Like the business objectives themselves, the policies and procedures are not static but are subject to innovation. As the well-respected management researcher and writer Peter Drucker noted,

> The purposeful innovation resulting from analysis, system and hard work is all that can be discussed and presented as the practice of innovation. But this is all that need be presented since it surely covers at least 90 percent of all effective innovations. And the extraordinary performer in innovation, as in every other area, will be effective only if grounded I the discipline and the master of it (Source: Peter Drucker, “Principals of Innovation” in *The Essential Drucker* (Harper Business, 2001).

The discipline of systems management can be mastered and the practice of systems management can be adapted and improved to meet the specific needs of different organizations.

The spectrum of systems management ranges from the reactive, uncontrolled ad hoc approach, through a controlled, procedure-guided method to an adaptive model built on well-defined controls that use performance measures to improve operations. Although there are many ways to organize systems management operations, one of the most promising for the complex heterogeneous IT environments of today is the SOM model.

Rationalizing Systems Management: SOM

Systems management is a discipline that can be mastered and perfected. To get to high-performance levels in systems management, organizations must implement policies and procedures that systematically define and control how changes are made, how new infrastructure is introduced, how systems are maintained, and a number of other areas. The diverse nature of systems management requires a classification scheme that allows you to organize the discipline into domains that can then be analyzed and optimized. For example, systems management includes both client management and security management. There are clearly overlap between the areas, but treating them as distinct operations will prevent you from being overwhelmed with the complexity of dealing with all the issues in both domains at once. One way of controlling the complexity is to think of systems management as a series of services that need to be delivered.

Elements of SOM

The domains of systems management can be viewed as services provided to users, applications, and the organization as a whole. These services are managed within an umbrella framework that is both modular and open. Some of the most important are:

- Service level management
- Financial management for IT services
- Capacity management
- Change management
- Availability management
- IT service continuity management
- Application management
- Software and hardware asset management

At first glance, these domains seem unrelated—such as financial management and change management—but they are all required for effective systems management and therefore must be included in any framework that purports to support the full breadth of demands in systems management. The details of these domains are beyond the scope of this chapter; instead, this chapter will examine the defining characteristics of a service-oriented architecture:

- Unified management framework
- Modular services
- Open architecture

📖 The details of how these services are managed are addressed in Chapters 4 through 8.

Unified Management Framework

A unified management framework is a common set of tools and services that support a variety of systems management operations. The centralized configuration management database is the best example of a constituent component of the unified management framework. Others include communication protocols, reporting systems, and client interfaces. As Figure 1.4 showed earlier aspects of different services are available from a single Web interface when a unified platform is used. Within the unified management framework, a series of modular services are available.

Modular Services

It is important to treat domains within systems management as distinct areas with their own set of requirements. For example, change management requires information about the state of software and hardware configurations throughout the enterprise. Before a port is closed on a firewall, a network administrator needs to know whether an application is using that port. This type of information is not required to manage the financial aspects of systems management and should be isolated from financial functions. At the same time, however, some of the configuration information has a definite impact on financial matters. For example, knowing the number and versions of OSs running within the organization is essential to managing licensing costs.

In addition to isolating information complexity, a modularized approach to systems management enables the framework to incorporate new services and management models as needed. A midsized company might not need capacity planning services initially, but as the company grows and the complexity of the IT infrastructure increases, manual methods for capacity planning may no longer be efficient or sufficient. For this reason, it is critical that a SOM framework be open.

Open Architecture

An open architecture is one that uses common, well-known protocols that are not proprietary to any one vendor or organization. In the world of systems management, an open architecture lends itself to incorporating multiple modules from a single vendor as well as leveraging services available from third parties. For example, a router vendor may provide data on router performance through the Simple Network Management Protocol (SNMP), which is collected in the centralized configuration management database, then integrated with other data collected from other network devices used in management reports generated by the systems management reporting module. By combining the benefits of a unified management framework, modular services, and an open architecture, organizations can realize the benefits of service-oriented systems management.

Benefits of Service-Oriented Systems Management

There are several benefits of service-oriented systems management beginning with improved understanding of the state of IT infrastructure and better control of that infrastructure. From there, organizations can realize improved cost effectiveness and improved QoS by standardizing infrastructure and procedures. With a centralized configuration management system in place, there are opportunities for automating manual processes—another area of potential cost savings. The benefits are not limited to just operation efficiencies.

Better systems management and standardized infrastructure and procedures lend themselves to improved security. When systems administrators can automate routine tasks—such as checking audit logs, distributing security patches, detecting which laptops are not running personal firewalls, and other mundane and time-consuming but essential, tasks—they have more time to spend on high-level security issues, such as risk management and compliance. As Figure 1.6 shows, the basic benefits enable organizations to meet higher-level needs as well as day-to-day operational requirements.

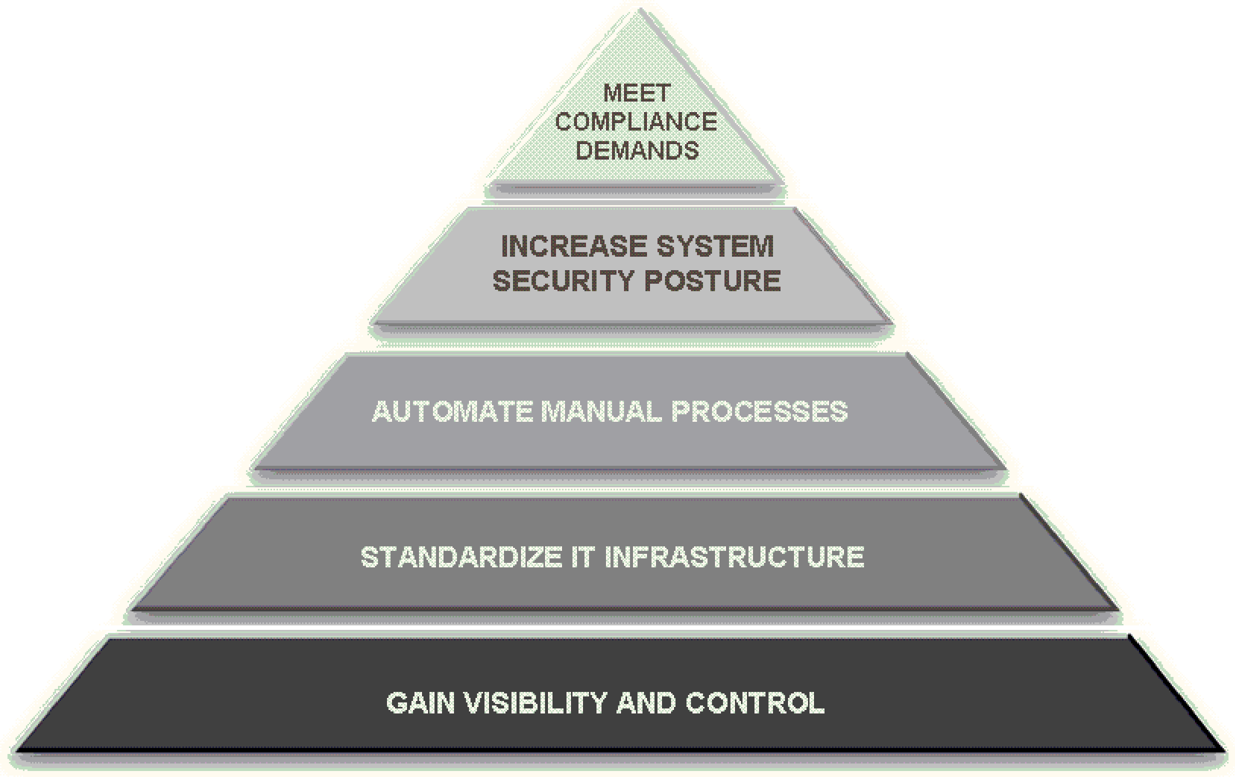

MEET
COMPLIANCE
DEMANDS
INCREASE SYSTEM
SECURITY POSTURE
AUTOMATE MANUAL PROCESSES
STANDARDIZE IT INFRASTRUCTURE
GAIN VISIBILITY AND CONTROL

Figure 1.6: Service oriented systems management enables organizations to meet both operational and strategic objectives.

Summary

Any organization with IT systems practices some form of systems management. How well they do so varies. The goal of systems management ultimately is to meet the strategic objectives of the organization, which include aligning with business operations, preserving the integrity of systems and information, and adapting to the changing needs of users. Systems management is a broad discipline with many domains; some of the domains are similar, some are less so. Underlying the entire practice, though, is a common set of information, processes, and procedures that are best managed as a unified whole. At the same time, the complexity of systems management requires a modularized approach to enable cost-effective and manageable solutions.

SOM builds on the best practices of systems management, information security, governance, and related areas. The remaining chapters of this guide will describe in detail the elements of these best practices, the tools needed to implement the best practices, and the organizational direction and policies needed to realize the benefits of SOM.

Download Additional eBooks from Realtime Nexus!