

realtimepublishers.comtm

The Reference Guide Totm

Data Center Automation



Don Jones and Anil Desai

Auditing	1
The Benefits of Auditing	1
Developing Auditing Criteria	2
Preparing for Audits.....	4
Performing Audits.....	4
Automating Auditing	5
Customers	6
Identifying Customers.....	6
Understanding Customers' Needs.....	7
Defining Products and Service Offerings	7
Communicating with Customers.....	8
Managing Budgets and Profitability	9
Total Cost of Ownership.....	10
Measuring Costs.....	10
Measuring TCO	12
Reducing TCO Through Automation	13
Reporting Requirements	13
Identifying Reporting Needs.....	13
Configuration Reports.....	13
Service Level Agreement Reporting.....	14
Real-Time Activity Reporting	15
Regulatory Compliance Reporting	15
Generating Reports	15
Using a Configuration Management Database	15
Automating Report Generation.....	16
Network and Server Convergence	17
Convergence Examples.....	17
Determining Application Requirements	18
The Roles of IT Staff	18
Managing Convergence with Automation	18

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Auditing

The process of auditing involves systematic checks and examinations to ensure that a specific aspect of a business is functioning as expected. In the financial world, auditing requires a review of accounting records, and verification of the information that is recorded. The purpose is to ensure that the details are consistent and that rules are being followed. From an IT standpoint, auditing should be an important aspect of operations.

The Benefits of Auditing

Although some IT departments have established regular auditing processes, many tend to perform these steps in a reactive way. For example, whenever a new problem arises (such as a security violation or server downtime issue), systems administrators will manually examine the configuration of a system to ensure that it is working as expected. A far better scenario is one in which auditing is performed proactively and as part of a regular process. There are many benefits of performing regular audits, including:

- Adhering to regulatory compliance requirements—Many companies are required to adhere to government rules or industry-specific practices. These regulations might specify how certain types of data should be handled or they might define how certain processes should be performed. In fact, many regulatory requirements necessitate regular auditing reviews to be carried out either by an organization or through the use of a third party.
- Verifying security—In many IT environments, security is difficult to manage. Every time a new server or workstation is added to the network, systems administrators must be careful to ensure that the device meets requirements specified in the security policy. Overlooking even one system could lead to serious problems, including loss of data. Additionally, IT departments must keep track of hardware and software licenses and ensure that users don't add new devices without authorization. By performing routine security audits, some of these potential oversights can be detected before they lead to unauthorized access or other problems.
- Enforcing processes—Auditing can help ensure that the proper IT processes are being followed. IT departments that have implemented best practices such as those specified within the IT Infrastructure Library (ITIL) can perform routine reviews to look for potential problems and identify areas for improvement.
- Change tracking and troubleshooting—Even in relatively simple IT environments, changes can have unintended consequences. In fact, many problems occur as a result of changes that were made intentionally. An auditing process can help identify which changes are being made and, if necessary, can help reduce troubleshooting time and effort.

These are just some of the important reasons for performing regular auditing of IT environments. The important point is that rather than being just a burden on an IT group, auditing can help ensure that the organization is working properly.

Developing Auditing Criteria

When working on developing auditing requirements and criteria, an organization should start by determining goals for the auditing process. The potential benefits already discussed are a good starting point. However, IT groups should add specifics. Examples might include *Sensitive customer data should always be stored securely* and *Change and configuration management processes should always be followed*.

Process-related criteria pertain to how and when changes are made and are designed to ensure that the intended IT service levels are being properly met. Organizations might develop auditing requirements to ensure that a process, such as manual server provisioning, is being performed correctly. These criteria often depend upon having well-documented processes that are enforced. For example, ITIL provides recommendations for steps that should be included in the change and configuration management process. Processes also pertain to standard operations in such areas as physical data center security, adherence to approvals hierarchies, and the definition of employee termination policies.

Configuration-related criteria focus on how workstations, servers, and network devices are set up. For example, security policies might require that all workstations and servers are only one version behind the latest set of security updates. Application-level configuration is also very important, as the strength of an IT organization's security system relies upon having programs up to date with regard to patches and user authorization settings.

Inventory-related auditing criteria generally involve verification that equipment is being tracked properly and that hardware devices are physically located where expected. Asset tracking methods and manual inspection of data centers and remote locations can help ensure that these criteria are being met.

Performance-related auditing criteria are designed to ensure that an IT department is providing adequate levels of service based on business needs. Metrics might include reliability, uptime, and responsiveness numbers. Furthermore, if the IT department has committed to specific Service Level Agreements (SLAs), those can serve as a basis for the auditing criteria.

Table 3.1 provides examples of auditing criteria and metrics that a typical IT department might develop.

Auditing Category	Auditing Purpose/Requirement	Metrics	Target
Process	Change management process must be enforced	Percentage of changes that obtained approval	
	100% of changes should be approved prior to being performed		
	All data center access is logged	Accuracy of data center entrance and exit logs	100% of data center visits are logged
Configuration	Servers are up to date with the latest security patches	Percentage of servers that are up to date based on security policy	100% of servers must be within one level of the latest security policy, and 50% must be running at the latest level
	CRM accounts are up to date	Only required accounts and permissions are in place, according to the IT CRM configuration policy	All permissions and user accounts should be consistent with IT and HR records
Performance	Ensuring adequate IT server and network uptime	Total unscheduled downtime (in minutes)	No more than 100% of the unscheduled downtime allowance, as specified in the SLA
	Service desk resolution times are within stated levels	Percentage of issues that are within times stated within the SLA	95% of tier-one issues should be resolved within 4 hours
Inventory	Asset tracking	Percentage of assets that are present according to previous audit results and change tracking details	100% of devices should be physically verified

Table 3.1: Sample auditing criteria.

Preparing for Audits

In many IT environments, preparing for an audit is something that managers and staff dread. The audit itself generally involves scrutinizing operational details and uncovering deficiencies. It also requires the generation of a large amount of information. The following types of information can be helpful in order to prepare for an audit:

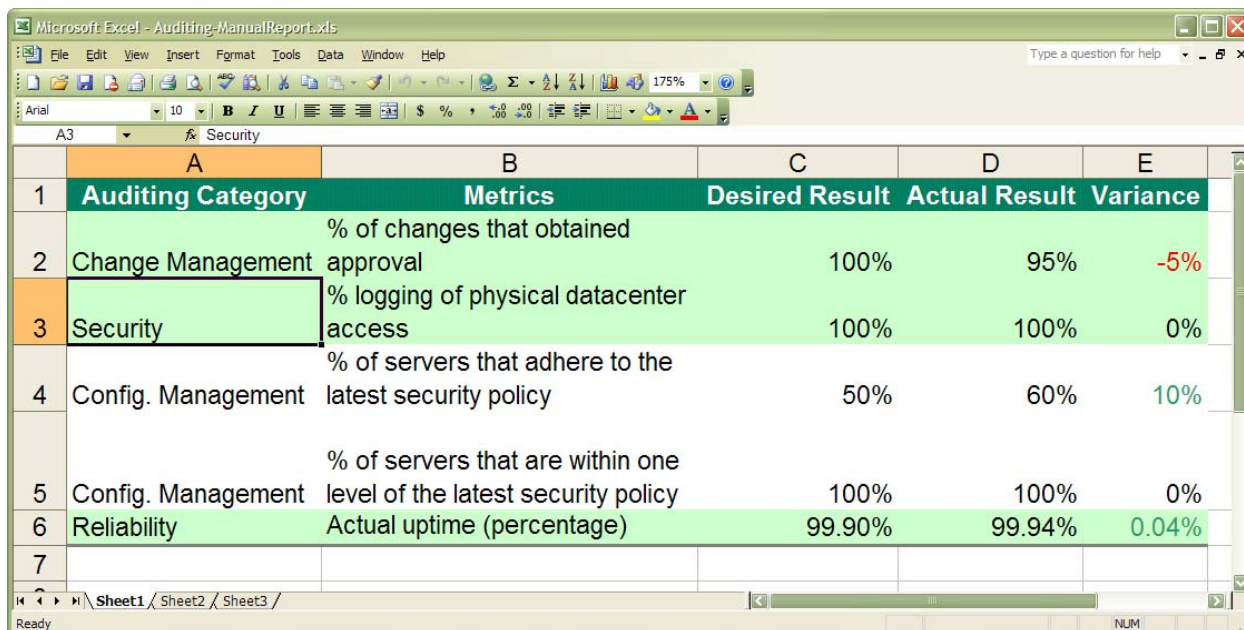
- Meeting minutes and details from regular meetings, such as change and configuration management reviews
- Asset inventory information, based on physical verification and any asset tracking databases
- Results from previous audits, in order to ensure that previous deficiencies have been addressed
- IT policy and process documents
- Information about processes and how they're enforced

All this information can be difficult to obtain (especially if done manually), but is often required in order to carry out auditing procedures.

Performing Audits

The process of performing an audit involves comparing the actual configuration of devices and settings against their expected settings. For an IT department, a typical example might be a security audit. The expected values will include details related to server patch levels, firewall rules, and network configuration settings. The employees that actually perform the audit can include members of the internal staff, including systems and network administrators and IT management. The goal for internal staff should be to remain completely objective, wherever possible. Alternatively, organizations can choose to employ outside professionals and consultants to provide the audit. This method often leads to better accuracy, especially if the consultants specialize in IT auditing.

Auditing can be performed manually by inspecting individual devices and settings, but there are several potential problems with this method. First and foremost, the process can be tedious and time consuming, even in small IT environments. Second, the process leaves much room for error, as it's easy to overlook a device or setting. Finally, performing routine audits can be difficult, especially in large environments in which changes are frequent and thousands of devices must be examined. Figure 3.1 shows an example of a manually generated auditing report. Although this report is far from ideal, it does show the types of information that should be evaluated.



	A	B	C	D	E
1	Auditing Category	Metrics	Desired Result	Actual Result	Variance
2	Change Management	% of changes that obtained approval	100%	95%	-5%
3	Security	% logging of physical datacenter access	100%	100%	0%
4	Config. Management	% of servers that adhere to the latest security policy	50%	60%	10%
5	Config. Management	% of servers that are within one level of the latest security policy	100%	100%	0%
6	Reliability	Actual uptime (percentage)	99.90%	99.94%	0.04%
7					

Figure 3.1: Manual spreadsheet-based auditing reports.

Automating Auditing

When performed manually, the processes related to designing, preparing for, and performing auditing functions can add a significant burden to IT staff. IT staff must be sure to define relevant auditing criteria, and they must work diligently to ensure that process and configuration requirements are always being met. Additionally, the process of performing audits can be extremely time consuming and therefore are generally performed only when absolutely required.

Fortunately, there are several ways in which data center automation tools and technologies can help automate the auditing process. One of the most important is having a Configuration Management Database (CMDB). A CMDB can centrally store all the details related to the hardware, software, and network devices in an IT environment, so it serves as a ready source against which expected settings can be compared. Asset tracking functionality provides IT managers with the power of knowing where all of their hardware and software investments are (or should be).

Change and configuration management tools can also help by allowing IT staff to quickly and automatically make changes even in large environments. Whenever a change is made, it can be recorded to the audit log. Furthermore, by restricting who can make changes and organizing the change process, data center automation tools can greatly alleviate the burden of performing auditing manually.

Although auditing can take time and effort to implement, the investment can quickly and easily pay off. And, through the use of data center automation tools, the entire process can be managed without additional burden to IT staff.

Customers

One of the many critical success factors for service-related organizations is customer service. Businesses often go to great lengths to ensure that they understand their customers' needs and invest considerable time and effort in researching how to better serve them. The customer experience can be a “make-or-break” factor in the overall success of the business.

Although the term “customer” is usually used to refer to individuals that work outside of an organization, IT departments can gain insight into the users and business processes they support by viewing them as customers. This shift in service delivery perspective can help improve overall performance of IT departments and operations for an organization as a whole.

Identifying Customers

An important aspect of service delivery is to define who customers are. In the business world, marketing organizations often spend considerable time, effort, and money in order to make this determination. They understand the importance of defining their target markets. IT departments can take a similar approach. Many IT departments tend to be reactive in that they respond to requests as they come in. These requests may range from individual user needs (such as password reset requests) to deployments of new enterprise applications (such as the deployment of a new CRM application).

The first step in identifying customers is to attempt to group them together. End users might form one group and represent typical desktop and workstation users from any department. Another group might be mid-level management, who tend to frequently request new computer installations or changes to existing ones. Finally, upper-level management often focuses on strategic initiatives, many of which will require support from the IT department. Figure 3.2 provides an example of some of these groups.

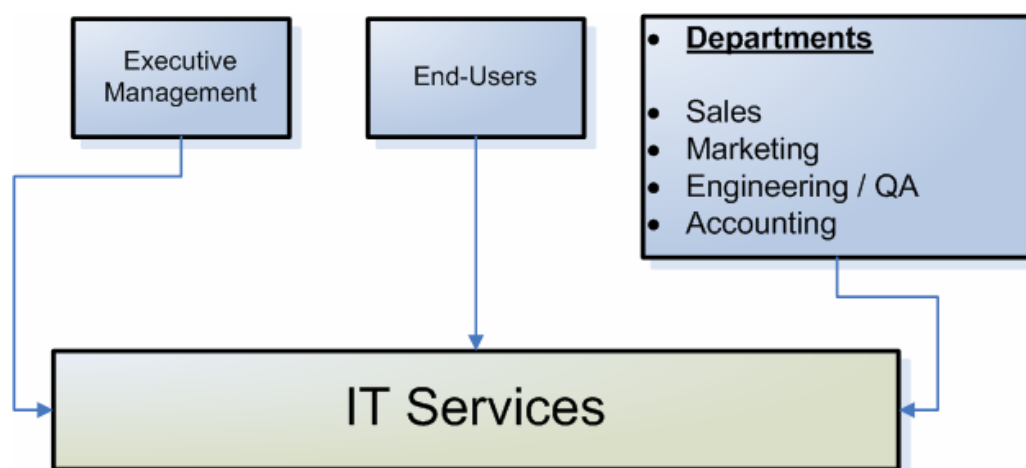


Figure 3.2: Identifying IT departments' customers.

Understanding Customers' Needs

Once IT departments' customers have been defined, it's time to figure out what it is they really need. In pre-sales discussions, traditional Sales staff will meet with representatives and decision makers to identify what their customers are looking for. They'll develop a set of requirements and then come back with a proposed solution. The key portion of this process is to have both business and IT representatives involved in the process.

It's important to be able to accurately identify "pain points" for customers—the areas that are causing them the highest costs and most frustrations. Often, IT departments tend to spend a significant portion of their time "fighting fires" instead of addressing the root causes of reliability problems. If IT management consistently hears that response times and service delivery delays are primary concerns, an investment in automation tools might help address these issues.

Defining Products and Service Offerings

Once their customers' needs have been identified, IT staff can start trying to find the best solutions to these problems. It is at this point at which the real benefits of the "customer-focused" model start to appear. Based on gathered requirements, IT management can start developing a set of service offerings to meet these needs. For example, if the Engineering department wants to be able to set up and deploy new machines as quickly as possible, investments in server virtualization and automated deployment tools might make sense. If reliability and uptime are primary concerns for several departments, investments in automated monitoring tools might make sense.

The best businesses find a way to offer standardized products or services that apply to many of their customers. Although it's often impractical to try to meet everyone's needs, the majority can often benefit from these offerings. Ideally, systems and network administrators will be able to find solutions that can benefit all areas of the organization with little or no customization. For example, developing standard workstation upgrade and deployment processes might be of interest to several different departments. True economies of scale can be realized when basic services become repeatable and consistent.

IT organizations can use several different practices to ensure that customers are getting what they "paid for." In some cases, Service Level Agreements (SLAs) can help define and communicate the responsibilities of the service provider. IT departments can commit to specific performance metrics and constantly track their success against these numbers. Data center automation tools can also be helpful in ensuring that SLAs are being met.

Communicating with Customers

An important aspect of overall success is related to vendors' ability to align their products and services with what their customers need. It's also important to recognize that, in some cases, what customers ask for might not be what they really want. By taking time to work in a "pre-sales" role to better identify the source of problems faced by customers, better solutions can be developed.

It's important to continue communications with customers, just as successful businesses work to earn repeated business from their existing client base. IT departments might find that their customers' needs have changed in reaction to new business initiatives or changing focus. This should serve as a good indicator that it might be time to hold a review and potentially update the products and services that are being provided. IT organizations should choose to restructure their offerings based on customers' changing needs. For example, if too many resources are currently allocated toward products or services that do not address major company initiatives, it will become obvious that these efforts could be better spent in another way.

The benefits of continued communications with customers are numerous. In the traditional business world, it's commonly understood that the value of keeping customers happy over time is high. Figure 3.3 shows an example of a continuing customer-focused process that involves "service after the sale."

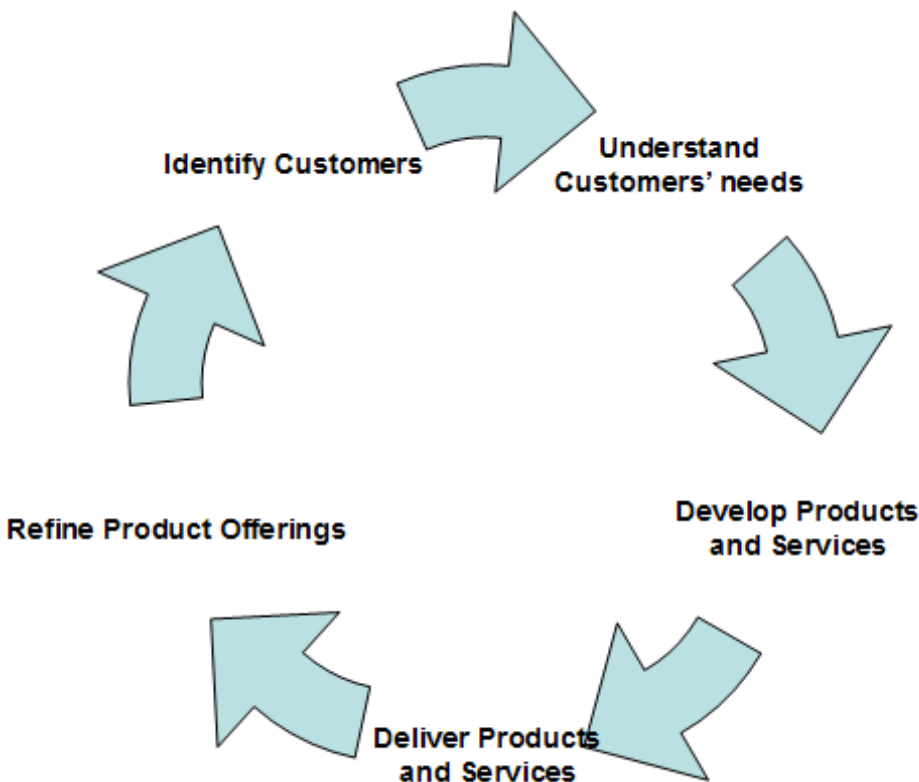


Figure 3.3: The customer-focused IT process cycle.

Managing Budgets and Profitability

Before a business can truly be considered successful, it must be able to show a profit—that is, its revenue must exceed its overall costs. In the case of internal IT departments, actual money might never change hands. And, the organization is typically structured to be a cost center.

Still, it's important to ensure that IT is delivering its products at the best possible price to customers while staying with budget. In some organizations, business and IT management may decide to implement this goal through inter-department charge-backs (a system by which the IT department will “charge” its customers and all expenditures will affect the budget of the department requesting products or services).

The goal of the IT department should be to reduce costs while maintaining service levels and products to its customers. This goal can often be achieved by increasing efficiency through the development of standard practices and the use of data center automation tools. Table 3.2 provides sample numbers that show how various technology investments can improve profitability.

Product or Service	Proposed Investment	Current Cost or Service Level	New Cost or Service Level	Benefit
Workstation deployment	Investment in automated deployment tools	\$350/workstation	\$90/workstation	\$270 savings per workstation deployed
Server deployment	Investment in automated server deployment and configuration tools	\$450/server	\$125/server	\$325 savings per workstation deployed
Average time to resolve basic Help desk issues	Purchase of automated Help desk system	~4 hours	~1.25 hours	Reduction in average resolution time by ~3.75 hours per issue
Server patch management	Automated security management solution	~ 12 hours per server per year	~ 2 hours per server per year	Reduction in time and effort required to maintain servers by approximately 10 years

Table 3.2: Improving IT product profitability.


Overall, there are numerous benefits that stand to be gained by having IT departments treat users and other business units as customers. By identifying groups of users, determining their needs, and developing products and services, IT organizations can take advantage of the many best practices utilized by successful companies. Doing so will translate into a better alignment between IT departments and other areas of the organization and can help to reduce costs.

Total Cost of Ownership

Determining total cost of ownership (TCO) involves enumerating all the time and effort-related costs in relation to implementing and maintaining IT assets. The main concept of TCO is that the initial purchase price of a technology is often just a very small portion of the total cost. Organizations benefit from getting a better handle on complete expenses related to their technology purchases and considering the many different types of charges that should be taken into account. This information will illuminate ways in which data center automation can help reduce costs and increase efficiencies.

Measuring Costs

Costs related to the management of IT hardware, software, and network devices can come from many areas. Figure 3.4 illustrates the types of costs that might be associated with a typical IT purchase.

 The numbers are hypothetical approximations and that they will vary significantly based on the size and amount of automation in various data center environments.

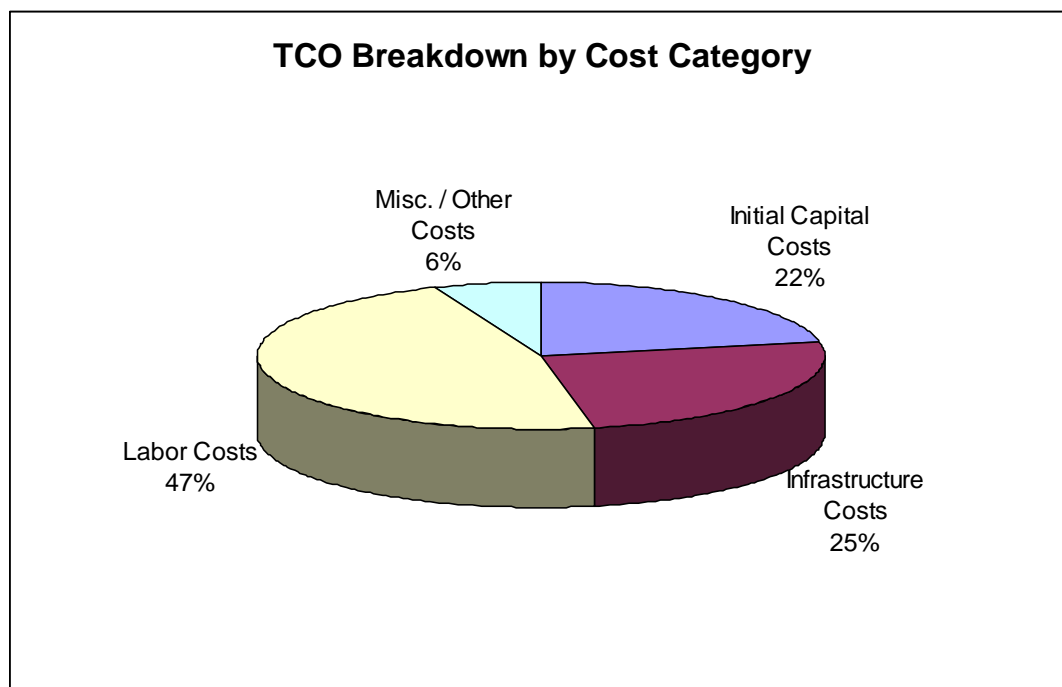


Figure 3.4: TCO breakdown by costs.

Identifying Initial Capital Costs

When asked about the cost of a particular product or service, IT staff will generally think first about the purchase or “sticker” price of the device. Servers, network infrastructure devices, and workstations all have very readily visible hard costs associated with them. The list of these basic costs should include at least the following:

- Capital equipment purchases—These costs are probably the ones that first come to mind for IT managers. For example, a new network-attached storage device might cost \$6500 to purchase. The charge is usually paid one time (at the time of purchase) and is related to the physical device or technology itself.
- Financing charges—IT organizations that choose to lease or finance the initial purchase price of capital assets will need to factor in financing charges. Depending on the terms of the lease, amounts may be due monthly, quarterly, or annually.
- Handling and delivery charges—Procuring new IT hardware requires basic transportation and handling costs. These are often included in part of the purchase transaction, but in some cases, additional delivery fees might be required.

Generally, these costs are easy to see. They will show up on invoices and purchase orders, and can be tracked by IT managers and accounting staff without much further research. However, they account for only one portion of the total cost.

Enumerating Infrastructure Costs

IT organizations should keep a close watch on ongoing costs that are related to supporting and maintaining the devices. Regardless of whether an IT organization owns its data center facilities, it will need to factor in costs for several areas of operation:

- Power—Costs related to electricity can represent a significant portion of total IT expenditures. Although it can be challenging to isolate the exact amount of power used by each device, average costs per amp of power can be calculated and distributed based on devices’ requirements. Power is required for basic functioning of the device as well as for cooling management. Furthermore, as the price of electricity can vary significantly, many financial predictions can partially hinge upon numbers that are outside an organization’s control.
- Support contracts and maintenance fees—Many IT hardware and software vendors offer (or require) support and maintenance contracts for their devices. These costs may be one-time additions to the purchase price, but generally, they’re paid through a monthly or annual subscription.
- Infrastructure costs—Whenever new IT equipment is deployed, physical space must be made for the new devices. Supporting infrastructure resources must also be provided. This infrastructure might include additional network capacity (switch ports and bandwidth), rack space, and any required changes to cooling and power capabilities.
- Network bandwidth—The implementation of new devices on the network will often require some incremental increase in network connectivity. Although additional costs are usually not required for every new device, total network-related costs should be distributed over all the workstations, servers, and networks that are supported.

By factoring in the ongoing support and maintenance costs, one more piece of the TCO puzzle is added.

Capturing Labor Costs

Once the initial purchase price of the physical device and related infrastructure is factored in, it's time to look at human resources. Labor-related costs associated with the entire life cycle of an IT purchase often account for a large portion of the TCO for a particular device. Typical areas include:

- **Selection**—The time it takes to evaluate various solutions and determine configurations can affect the overall cost of an IT investment.
- **Deployment**—After equipment is delivered, labor is required in order to physically “rack” the new device and to configure it for use. Some cost reductions can be realized when installing numerous devices at the same time.
- **Configuration and testing**—New computers and network devices rarely come from the factory completely ready for use. Initial configuration often requires significant time, especially if it is a new device with which the IT department is unfamiliar. Testing is critical in order to ensure a smooth deployment experience.
- **Systems administration**—Application and operating system (OS) updates, performance monitoring, security management, and other routine tasks can add up to significant ongoing computing costs.
- **Replacement**—It's no secret that all IT investments have limited useful life spans and must be replaced eventually. The cost of removing and replacing old hardware should be factored into the total cost.

To calculate labor-related costs, IT managers should group their employees into specific skill areas and determine average per-hour costs for those personnel. In many cases, it might make more sense to determine an average value for the number of hours spent on certain tasks. Some tasks, such as fixing hardware failures, may be performed infrequently, and only on a few machines in the environment. For these cases, IT management can calculate the total number of hours spent repairing hardware problems, then divide that by the total number of servers in the environment. The result is a useful “cost per server” amount that can then be factored into other technology decisions.

Measuring TCO

There are many challenges that IT organizations will face when trying to calculate TCO for the devices they support. The main problem is in determining cost-related numbers. Some of this information can come from reports by IT staff, but that data is often incomplete. Asset management tools can greatly help keep track of “hard costs,” especially those related to new purchases. These tools generally allow factoring in finance costs, operating costs, and depreciation—all of which can be important for determining TCO.

A good source for labor-related costs can be an automated Help desk solution and change and configuration management tools. IT staff can easily report on the amount of time they've spent on specific issues by using these tools.

Reducing TCO Through Automation

Many of the real costs related to technology investments are related to deployment and ongoing management. Data center automation tools can greatly help in measuring and reducing TCO. By providing reports of the time and effort required to maintain servers, workstations, and network devices, IT managers can get a more accurate picture of total costs.

Once an organization has a good idea of where its major operational costs are coming from, it can use this information to start reducing those costs. Most IT organizations will find that they spend significant amounts of money on basic labor-intensive operations that can be quickly and easily automated through the use of the right tools. For example, if a major cost component related to supporting servers is deployment, automated server provisioning tools can help lower those costs. Similarly, if a large portion of the expenses come from ongoing maintenance, automating monitoring, change, and configuration management solutions can help dramatically. Overall, by keeping in mind the components of TCO, IT departments can make better decisions related to managing and lowering the costs associated with service delivery.

Reporting Requirements

An old management saying states that “If you can’t measure it, you can’t manage it.” The idea is that, without knowing what is occurring within the business, managers will be unable to make educated decisions. This idea clearly applies to IT environments, where major changes happen frequently and often at a pace that is much faster than that of other areas of the business. That is where reporting comes in—the goal is for IT management to be able to gain the insight they need to make better decisions. It is useful to know what types of reports can be useful, and how these reports can be generated.

Identifying Reporting Needs

The first step in determining reporting requirements is to determine what types of information will be useful. Although it’s tempting for technical staff to generate every possible report (just because it’s possible), the real initial challenge is in identifying which information will be most useful.

Configuration Reports

Configuration reports show IT managers the current status of the hardware, software, and network environments that they support. Details might include the configuration of specific network devices such as routers or firewalls, or the status of particular servers. Basic configuration information can be obtained manually through the use of tools such as the Windows System Information Application (as shown in Figure 3.5).

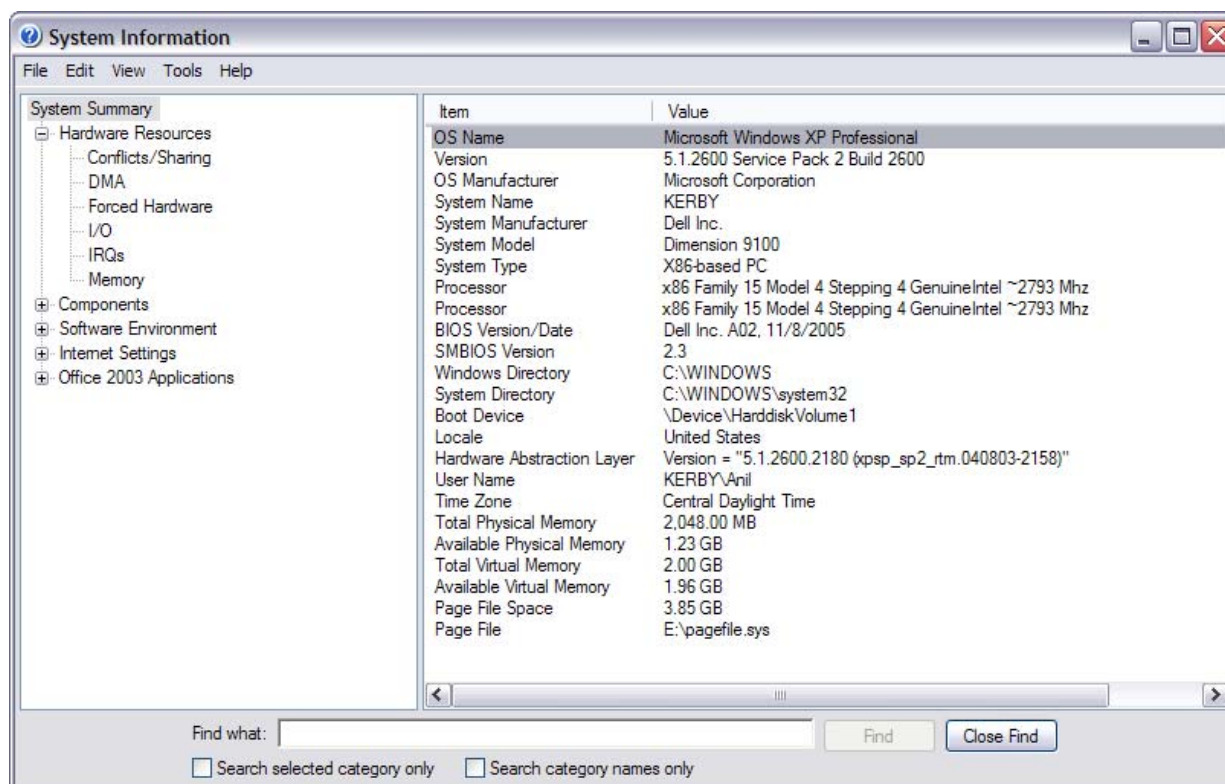


Figure 5: Viewing configuration details using the Windows System Information tool.

These reports can be very helpful by allowing IT managers to identify underutilized resources, and for spotting any potential capacity or performance problems. They are also instrumental in ensuring that all systems are kept up to date with security and application patches. Reporting solutions should be able to track assets that are located in multiple sites (including those that are hidden away in closets at small branch offices) to ensure that nothing is overlooked.

Service Level Agreement Reporting

An effective method for ensuring that IT departments are meeting their users' needs is through the use of well-defined Service Level Agreements (SLAs). An SLA might specify, for example, how much downtime is acceptable for a specific application, or it might define an expected turnaround time for the deployment of a new server. These agreements can affect operations throughout the business, so IT managers generally want to keep a close watch on them. SLA reporting features will allow IT staff to specify thresholds for specific metrics (such as server deployment time), then provide for the creation of reports that show the expected values compared against the agreed-upon values. These reports can also be helpful in improving the perception of IT throughout an organization (assuming, of course, that service levels are met).

Real-Time Activity Reporting

Most IT departments are characterized by rapid changes in short amounts of time. Many of these changes occur in reaction to changing business requirements; others are performed in order to improve the IT infrastructure. It can be very difficult to keep track of all of the changes that are occurring on workstations, servers, network devices, and applications. In this arena, real-time reporting can help. The information in these reports is always kept up to date and can be referenced many times during the day. Ideally, the reports will include details about what changed, why the change was made, and who performed the change. This information can greatly assist business and technical staff in coordinating their activities and troubleshooting problems.

Regulatory Compliance Reporting

Many industries are required to comply with government and industry-specific regulations to ensure that their operations are within guidelines. Examples include the Sarbanes-Oxley Act (for public companies) and the Health Insurance Portability and Accountability Act (HIPAA—for the healthcare industry). They must not only follow the rules but also be able to prove it. Regulatory compliance reports generate information related to the metrics of the current IT environment, then compare this data against specific regulatory requirements. With this information, IT management can quickly identify any deficiencies that must be resolved.

Generating Reports

Once an organization has determined the requirements for its reports, it can start looking at how the reports can be generated. There are many ways in which report creation and generation can be simplified.

Using a Configuration Management Database

Determining the source of reporting data can be difficult in many IT organizations. Data tends to be stored in a variety of different “systems,” including paper-based records, spreadsheets, custom database solutions, and enterprise systems. It can be very difficult to bring all this information together due to differences in the types of data and how information is structured. By using a centralized Configuration Management Database (CMDB), IT departments can store the information they need within a single solution. This data store greatly simplifies the creation and generation of reports, and can help ensure that no information is overlooked (see Figure 3.6).

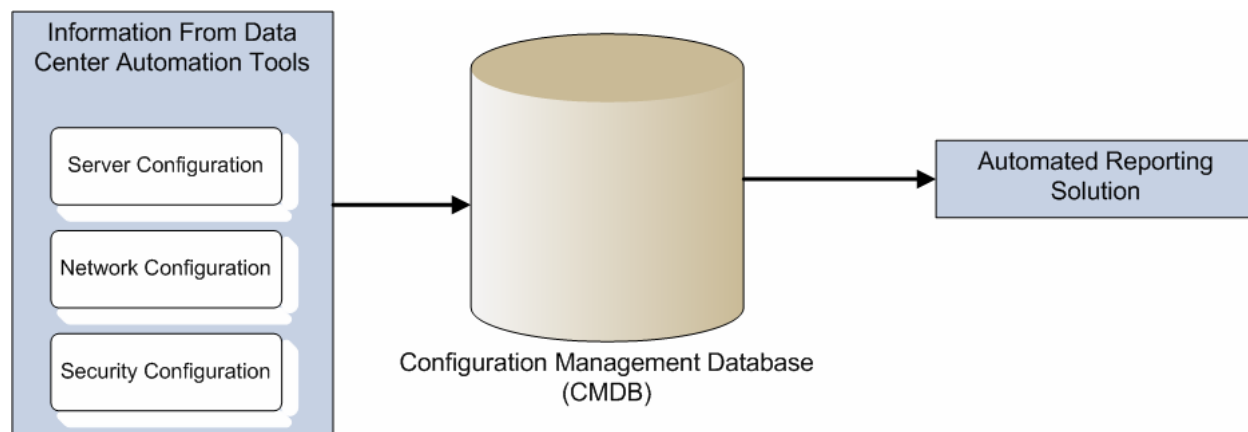


Figure 6: How a CMDB can help facilitate reporting.

Automating Report Generation

One of the challenges related to many types of reporting is that, as soon as the report is generated, it's out of date. Fortunately, electronic report distribution methods can help alleviate this problem. Automated IT reporting solutions can provide numerous features:

- **On-demand reporting**—Whenever necessary, users should be able to generate up-to-the-second reports on-demand. This type of reporting is particularly useful when managers want to closely track information that might change during the day. In larger IT environments, reports might take a significant amount of time to generate, so scheduling options can be helpful.
- **Automatic report distribution**—Many business processes revolve around regular meetings and review processes. Automated reporting solutions that have the ability to automatically send reports based on a predefined schedule can help ensure that everyone is kept up to date. Reports can be distributed via an intranet site or through email.
- **Alerts**—IT managers often expect their staff to notify them if some aspect of the organization needs special attention. The same requirement is true for reporting. Reporting solutions can provide the ability to set alerts and thresholds that can highlight particularly important or interesting aspects within reports. For example, if downtime has currently exceeded the limits specified by the service level for the Engineering department, IT managers could have the report highlight this in red.

Overall, through the use of automated reporting, IT departments can gain the information they need to make better decisions about their business and technical operations. The result is reductions in cost and improvements in service levels.

Network and Server Convergence

Over time, IT applications have evolved to become increasingly reliant on many components of an IT infrastructure. In the past, it was common for even enterprise-level applications to be hosted on one or a few servers, and many organizations' networks were centralized. The job of the network was to ensure that clients could connect to these servers. Modern enterprise applications are significantly more complex and often require the proper functioning of dozens of different portions of an IT environment to be working properly. Server and network management have converged to a point at which they're highly inter-dependent.

Convergence Examples

In typical IT environments, there are many examples of devices that blur the line between network and server operations. Dedicated network appliances—such as network-attached storage (NAS) devices, firewalls, proxy servers, caching devices, and embedded Web servers—all rely on an underlying OS. For example, although some NAS devices are based on a proprietary network operating system (OS), many devices include optimized versions of Windows (such as the Windows Storage Server) or Linux platforms. Figure 3.7 shows an example of this configuration.

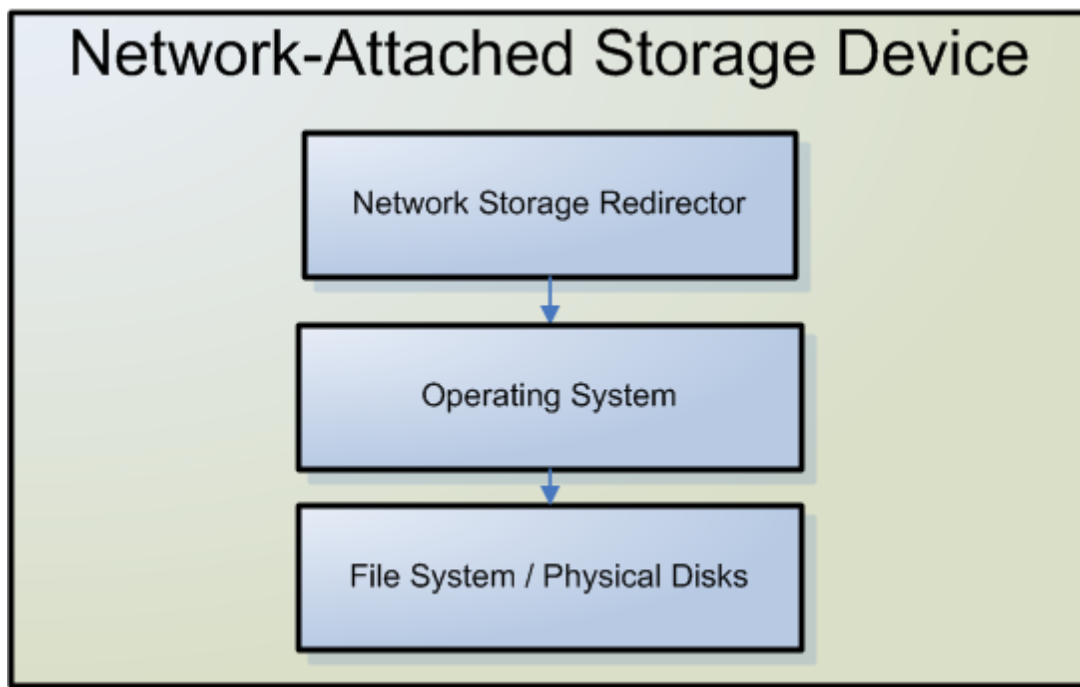


Figure 3.7: Components of a typical NAS device “stack.”

In many of these systems, there are clear advantages to this type of configuration. For example, several major firewall solutions run on either Windows or Linux platforms. The benefit is that systems administrators can gain the usability features of the underlying OS while retaining the desired functionality. From a management standpoint, however, this configuration might require a change to the standard paradigm—to ensure that the device is performing optimally, network and systems administrators must share these responsibilities.

Determining Application Requirements

One of the most important functions of IT departments is ensuring that users can access the applications they need to perform their jobs. The applications themselves rely on server resources as well as the network. An important first step in managing this convergence is to identify the requirements that applications may have. Table 3.3 provides an example of some typical types of applications and their dependencies.

Application	Servers Required	Networks Required
CRM	AppServer01, WebServer01, DatabaseServer01	VPN access for all branch offices and traveling users
Engineering/QA Defect Tracker	Engineering01, Engineering03, EngineeringDB05	Engineering network Internet access and VPN access (home users)
Intranet	IntranetServer01 (cluster), KnowledgeMgmtDB	Corporate LAN, branch office WANs, and VPN

Table 3.3: Identifying application requirements and dependencies.

By highlighting these requirements, IT staff can better visualize all the network and server infrastructure components that are required to support a specific application.

The Roles of IT Staff

In the past, IT operations tended to be specialized in numerous isolated roles. A typical staff might include network specialists, database specialists, server administrations, and application managers. It was often acceptable for each of these administrators to focus on his or her area of expertise with limited knowledge of the other areas. For most modern IT organizations, this structure has changed. Systems administrators, for example, often need strong network skills in order to complete their job roles. And application developers must take into account the underlying network and server infrastructure on which their programs will run.

Unfortunately, it's impractical to expect all IT staff members to have strong skills in all of these areas. To address this issue, IT departments must rely on strong coordination between the many functional areas of operations to ensure that applications can remain functioning properly.

Managing Convergence with Automation

When handled manually, it can be challenging for IT staff to develop the levels of coordination that are required to ensure that converged applications are managed properly. However, many of the features of data center automation tools can help. First, by storing network- and server-related configuration details in a single Configuration Management Database (CMDB), IT staff can more easily see the inter-dependencies of the devices they support. Change and configuration management tools can help ensure consistency in how these devices are managed. Overall, the IT staff can better manage the complexity resulting from the convergence of network and server management through the use of data center automation tools.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.