Realtime publishers
"Leading the Conversation"

The Definitive Guide™ To

Service-Oriented Systems Management

sponsored by

altiris®

Dan Sullivan

Copyright Statement

Chapter 12: Roadmap to Implementing Service-Oriented Systems Management Services

Service-oriented management is the platform for managing systems management functions across the diverse and wide-ranging needs of today's enterprises. The platform takes a function- rather than device-specific focus for several reasons:

- The need to stay aligned with business objectives requires an agile management structure
- Demands on IT management, such as compliance, apply to IT services not to specific devices
- Devices accessing enterprise resources may be managed (owned by the enterprise), semi-managed (owned by employees but subject to some IT policies, such as smartphones), or unmanaged, such as public kiosks and customer PCs that access Internet-accessible services

The evolution of service-oriented management is driven by the demands placed on IT managers and systems administrators; some of the most prevalent are:

- Responding to new market opportunities
- Reducing IT operations costs
- Sharing information and assets with business partners
- Making network resources accessible from remote locations
- Providing more services to customers online
- Meeting emerging requirements of auditors and regulators

Each of these drivers is a bridge point between business and IT operations. None of these are exclusively business or technical. The divisions between the technical and non-technical (or business) sides are fast becoming a legacy of earlier times. This chapter provides a roadmap for implementing service-oriented management by examining four topics:

- Limits of traditional management models in light of emerging challenges in systems management
- Current status of IT operations
- Transition to mature service model
- Implementation of a service model for systems management

As noted earlier, evolving demands on IT are bringing IT and business operations closer than they have been in the past.

Limits of Traditional Management Models and Emerging Challenges

Some may wonder why systems management practices need to change, but the fact is that the demands on IT are evolving just as much as the underlying technology.

Demise of Device-Centric Systems Management

Traditional management models that focused on fixed functions or OSs for devices may not fit neatly with the way devices are deployed and reused in today’s environments. For example, there was a time when it might make sense to divide management duties for specific devices based on the types of OS deployed. This might include:

- Windows desktops, running Windows 98 or other desktop-only system
- Windows servers running email and network file servers
- Linux servers that ran Web servers, ftp servers, and other low-demand systems
- UNIX servers for high-end operations, such as database servers

Today, similar Windows systems run from notebooks to servers with dual-core processors just as likely in desktops as servers. Linux servers are now just as likely to host full relational database systems as UNIX platforms are. And devices are not even limited to single OSs—virtualization allows multiple different OSs running concurrently on a single machine.

The management tasks associated with the range of devices is also consolidating into several well-understood areas:

- Procuring
- Deploying
- Patching
- Monitoring
- Securing
- Retiring

The kinds of information that must be tracked and operations performed do not vary by operating system or hardware manufacturer.

Example Benefits of Service-Oriented Management

With this evolution of systems management practices comes some beneficial new practices. For example, you can now effectively track virtually all IT hardware assets in a configuration management database (CMDB). A single logical repository can provide more efficient access to information about the state of an organization's infrastructure than if the information were along the lines of platform type or assigned managers.

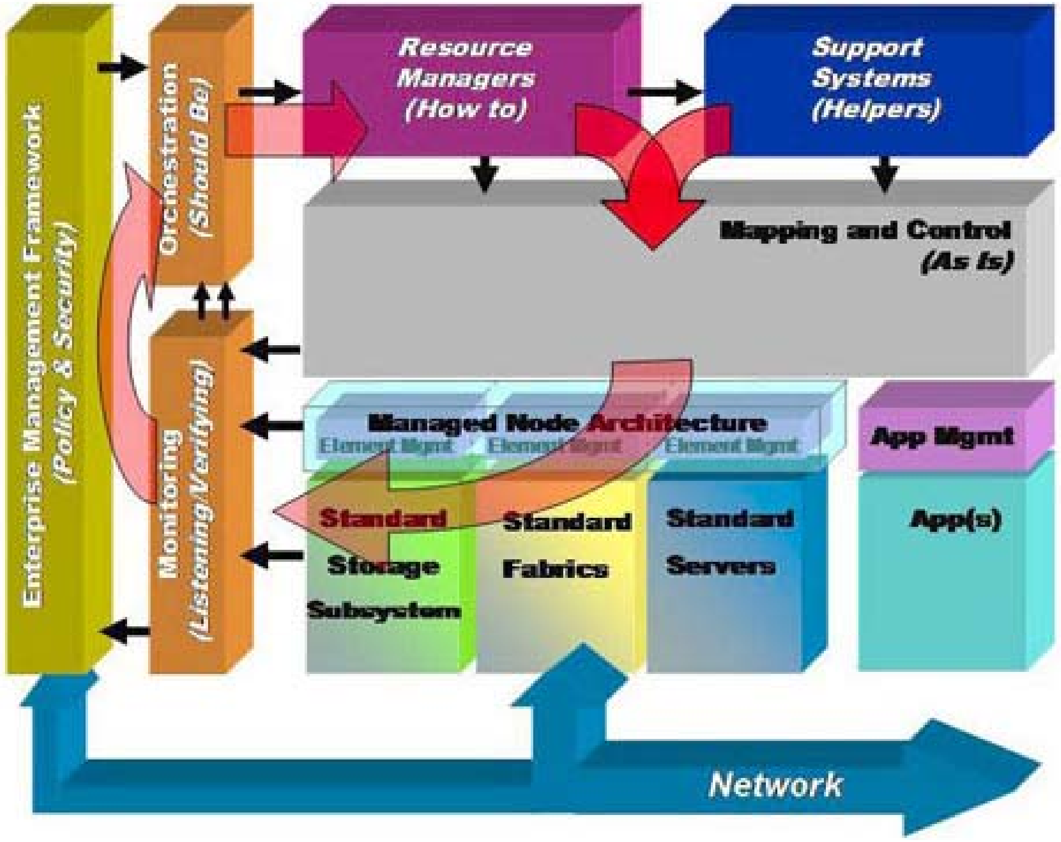

Figure 12.1: CMDBs provide the means to track virtually all IT assets.

A CMDB captures four types of information:

- Standards and baseline
- Technical
- Ownership
- Relationship

Technical details vary by the type of configuration item. For example, hardware technical data can include model numbers, firmware versions, storage capacity, and other physical attributes. Software applications may include version numbers, patch levels, and administration documentation.

Ownership information tracks the organizational dimension of a configuration item. This can include the business unit responsible for the services provided by a configuration item. For example, the finance department may be the owner of a server and enterprise resource planning (ERP) application. Ownership may be distinct from responsibility, which should also be tracked in a CMDB. A group within the IT department may have responsibility for the application server owned by the finance department in the previous example.

Relationship data describes how configuration items depend on one another or are used together. For example, a UNIX server may depend on a particular router in the network.

Take the case of a newly discovered piece of malware that exploits a vulnerability in a commonly used code library. Which devices in the organization are using that library? Of all the vulnerable devices, which are running mission-critical operations? Which are on mobile devices that may not be connected to the network and may not receive the patch when pushed to devices by the patch management system?

Compliance is forcing a new regimen on IT operations. More controls are now required to ensure that devices are configured properly and patched appropriately. It is not uncommon to establish minimum security requirements for any device connecting to the network. Notebooks, for example, may be required to run anti-malware and personal firewalls. If these services are not available, the device is not granted access to the network. How is this enforced?

Policy management solutions and access control devices have to be coordinated to ensure any device accessing the network is in compliance. A single policy can apply to multiple devices and devices may be subject to multiple policies. The responsibilities of systems managers are growing rapidly and automation is essential to keeping up with these changes. If automated systems management solutions are not in place, or partially in place, the first step is to assess the state of IT management practices.

Roadmap Step 1: Assessing the Current Status of IT Practices

IT practices are so wed to the particulars of the technology deployed in an organization that it is easy to underestimate the importance of the business drivers behind IT operations. For this reason, the first step in preparing for the move to a service-oriented model of systems management is to understand the following:

- Overall business strategy and goals
- The state of IT alignment with business strategy
- The risk tolerance of the organization

The purpose of this step is to ensure that the technical decision making in later stages is done in a way that supports the broad objectives of the organization.

Overall Business Strategy and Goals

This may sound obvious, but then again, starting at the beginning always does. The first step in the move to service-oriented strategies is understanding the strategy and goals of the organization. Of course, if the organization is a commercial entity, the goal is to make a profit and increase shareholder value; if the organization is a government agency, the goal is to serve the agency's constituency. That is the obvious part; the less obvious part is how to do it.

Executive management sets goals and strategies that answer the "how" question. For example, a company may have the goal of increasing market share in a particular region and will do it by improving customer service. An agency may decide that it will improve service to its constituency by reducing the cost of delivering three high-volume service transactions. These are the kinds of goals that IT manager can take as guides to formulating IT plans; they are in essence the functional goals that IT, in conjunction with other departments, must deliver. An important aspect of this process is prioritizing support offerings, controlling support costs, and in some cases, outsourcing low-end priorities. Making sure IT managers understand functional goals and keeping IT operations in sync with those goals is an ongoing process.

IT Alignment and Business Strategy

Clear definition of business goals coupled with communication about those goals is the basis of IT alignment with business strategy. Some challenges with keeping IT and executive direction in sync include:

- Bridging the business and technical parts of an organization due to difficulties translating from business goals to technical implementations
- Including IT in planning changes in business direction; for example, a shifting emphasis to new markets, product lines, or business models
- Keeping business managers aware of changes in technical implementations, such as resource limitations, development cycles, and changes to delivery schedules of new systems or modifications to existing systems

Ironically, it is often not technical problems but communication problems that can cause the greatest difficulties at this level. However, one of the advantages of a service-oriented management model is that operations are managed at a higher level of technical abstraction that more easily aligns to business operations. This can contribute to more effective communications between business managers who might describe goals and problems in terms of services and technical managers who can now measure and control operations in terms of those same services.

Bridging the gap between business and technology concerns and objectives requires a sound understanding of both realms. Meeting business requirements often requires staffing IT operation with business analysts along with technical professionals.

The final piece of the first step of the roadmap is assessing the risk tolerance of the organization. As Figure 12.2 shows, goals and executive strategies may drive IT operations, but all these decisions are made within a particular and organization-specific environment for risk and risk tolerance.

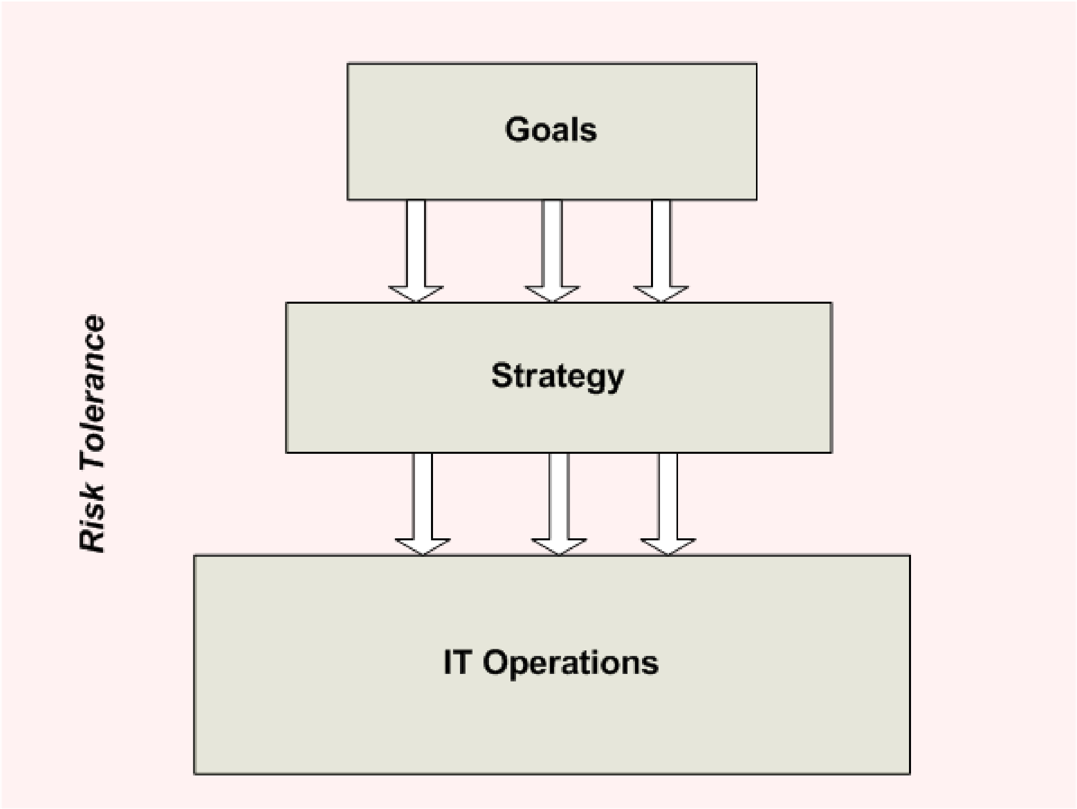

Figure 12.2: Risk tolerance is part of the background in which all business and technical decisions are made.

Risk Tolerance of the Organization

Well-formulated goals and strategies for achieving those goals are necessary but not sufficient to guide IT decision making; another required piece is an understanding for the risk tolerance of the organization. No strategy can guarantee success—there will always be unknowns and uncontrollable events that thwart best efforts. Take for example, a large-scale migration to Microsoft Vista. Although best practices, such as the Business Desktop Deployment guidelines, can help with the planning and assessment, the potential for problems still exist. Risks include operational downtime due to software incompatibilities, insufficient hardware, errors in establishing access controls, and insufficient service desk resources.

> 📖 For more on Vista migration, see the Microsoft Desktop Deployment Center and the Altiris Vista Resource Center.

A formal risk analysis can identify the theoretical cost and benefits of risks and risk mitigation strategies. Of course, executives and managers will try to mitigate these risks but there are limits to these efforts:

- Financial constraints
- Time constraints
- Unknown factors
- Unknown frequencies of risks
- Technical limitations
- Resource constraints

Understanding these limitations and working around them must be guided by the organization's tolerance for risk.

Financial Constraints

Managers have limited resources for dealing with risks and choices will often have to be made between mitigation strategies. For example, should funds be invested in a new higher-capacity backup system or should those same funds be used to upgrade network security? Both are arguably essential to maintaining business operations, but there may be funds for only one.

> ✎ Investment options can be measured in several ways:
>
> - Return on investment (ROI)
> - Internal rate of return (IRR)
> - Net present value (NPV)
> - Payback period
>
> Alternatively, several methods may be used in combination, much as with the balanced scorecard model.

Time Constraints

Time constraints are also a factor. One may have the funds and staff with the technical skills to address a problem but not the time. If a company acquires another firm with poorly designed network architecture, should the new resources be redeployed following the company's architecture? Ideally yes, but it may require pulling senior systems administrators and network managers away from other high-priority projects.

Unknown Factors

There is little one can do about unknown factors except to plan in terms of broad generalities. Natural disasters, security breaches, and systems failures are broad risks but you will never be able to plan in detail for all types or understand the impact of all possible instances of these risks.

Another class of unknowns is the impact of risks. A fire that destroys a computer center is easily quantified. The cost of a data loss incident is not so clear, but key factors include:

- Diminished brand value
- Loss of customer loyalty
- Fines and other compliance costs

In addition to these kinds of unknowns, another group of unknowns add to risk assessment difficulties.

Unknown Frequencies of Risks

Weighing the impact of risks requires understanding the expected frequency of those risks occurring. For example, if an IT center is built on a 50-year flood plain, one can estimate the expected cost of the risk associated with floods.

Unfortunately, not all risks are so well understood. For example, there is little historical evidence to estimate the probability of a successful breach of database security and the theft of customer financial information. There is anecdotal evidence from isolated incidents but without measures of the full breadth of breaches and details of each breach, it is difficult to assess the frequency.

In such situations, the risk tolerance of an organization is the best guide. Are executives willing to invest $100,000 in new security measures to prevent a database breach? How about $1,000,000? Defensive investments can be difficult to justify because there is always the chance that they will never be required.

Technical Limitations

For some risks, you simply do not have adequate mitigating solutions. Information security has always been a matter of responding to emerging threats that are motivated to circumvent existing countermeasures. Some of the best methods for dealing with known risks impose unacceptable limitations. For example, Windows Vista has been designed with improved security measures but some existing software will not function under these new security measures. Users have a choice to not run these applications or to run them with elevated privileges that provide similar access to earlier versions of the Windows OS. As Figure 12.3 shows, what is desired and what is achievable can be vastly different because of the constraints facing the organization.

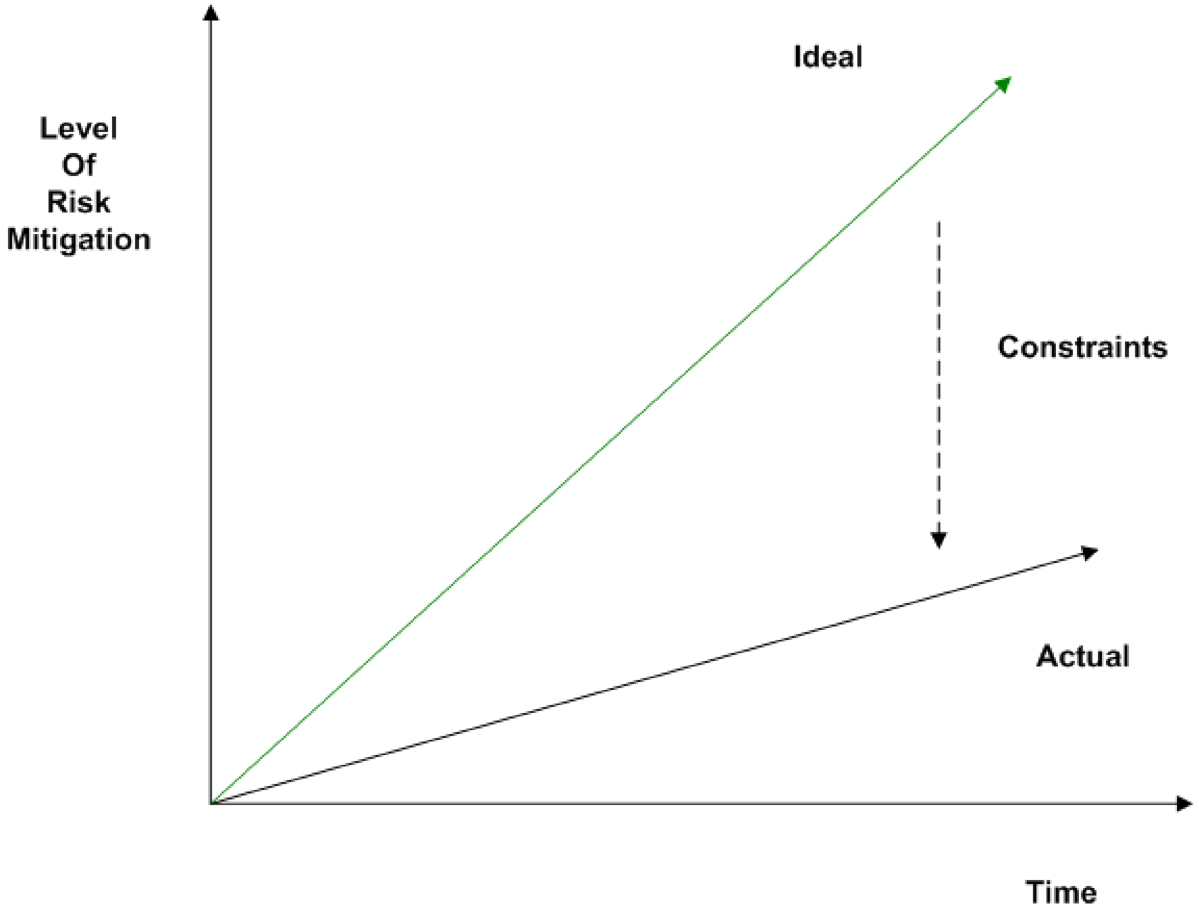

Figure 12.3: A variety of constraints limit an organization's ability to reach the ideal level of risk mitigation.

Resource Constraints

Another constraint is the availability of resources, especially staff with sufficient skill sets. Again, planning can mitigate some of these risks but there is always the potential for a key person to leave a project at a critical time.

Responding to Risks

Once risks have been identified, an organization can respond to those risks in one of three ways:

- Accept the risk
- Mitigate the risk
- Transfer the risk

Accepting the risk means the organization understands the risk, has evaluated the potential costs of the risk as well as the costs and benefits of deploying countermeasures to the risk but has decided not to take any steps to reduce the risk. At first glance, this may sound somewhat irresponsible, but this is often a reasonable strategy. For example, if a data center is in a 100-year flood plain, a company may decide that moving the operation or deploying flood controls outweighs the benefits; accepting the risk is then a reasonable strategy.

Mitigating the risk means that countermeasures are taken to reduce the risk. You use risk mitigation strategies constantly, although you may not think of them as such. Consider the following:

- Deploying anti-malware on PCs
- Implementing content filtering on network traffic
- Establishing acceptable use policies for IT equipment
- Using clusters of computers instead of a single server for a mission-critical applications
- Conducting code reviews on custom-developed applications
- Using project management best practices

These are all examples of risk mitigation measures. Some of these, such as deploying anti-malware programs, are obviously done to reduce a well-known risk. Others, such as project management best practices, are not solely risk mitigation measures although it is a key proactive risk mitigation technique. In the case of project management, the best practices reduce the risk of cost overruns and delay of deliverables. Risk mitigation does not eliminate risks; that is not possible. Instead, the goal is to reduce the risks as much as possible using reasonable resources.

The final option for dealing with risk is to transfer it. This means an organization purchases insurance so that in the event the risk is realized, the insurance company bears the cost of the risk. Like risk mitigation, risk transfer is appropriate in a variety of circumstance and its use will depend on the balance of cost and benefits.

At the conclusion of step one, an organization should have an understanding of business objectives and how IT can serve those objectives. At the same time, these steps provide some perspective on risks and the ability to mitigate those risks. The next step is specific planning for a move to a service-oriented model.

Roadmap Step 2: Planning Transition to Mature Service Model

The first step in the roadmap to implementing a service-oriented management model is largely preparatory. It is akin to deciding where you want to go before you get in the car and start driving. In step 2, you are still not driving but are planning how to get where you have decided to go. The planning process consists of three core operations:

- Prioritizing needs
- Building a central management foundation
- Optimizing policies and procedures
- Creating an alternative, backup plan

Let’s begin with a review of the landscape of services that must be provided.

Prioritizing Needs

Service-oriented management and systems management in general encompass a wide range of operations and services. The first part of the planning process is to understand which of these operations and services are the most important; common among top priorities are:

- Acquiring devices and applications
- Deploying devices and applications
- Providing service desk support
- Ensuring asset management
- Maintaining systems availability
- Monitoring systems
- Auditing and compliance reporting
- Developing applications
- Securing databases and hosts
- Enforcing policies
- Improving quality controls on IT procedures
- Ensuring application compatibility

Each of these could justifiably be considered top priorities depending on the circumstances. There is no single right answer to the question, “Where should we start?” Rather than try to force a one-size-fits-all answer to that question, it may be more useful to examine a few scenarios to see how varying circumstances shift priorities. These will include:

- A new business without an existing systems management structure
- A company that has recently acquired another firm
- A company in a highly regulated market

Again, the goal is not to provide a black-and-white decision-making procedure for how to proceed with prioritizing needs but to show some examples of the kinds of questions and issues that may influence the prioritization process.

New Business

Consider a new business that is started to provide online services to manufacturers. The services are delivered through a combination of onsite consulting and online support through a customer portal. (The details of the service are not important at this point.) The characteristics of the market are:

- Relatively few compliance requirements because the customers are not in financial services, healthcare, or another highly regulated area
- The company is privately held so the Sarbanes-Oxley Act (SOX) does not apply
- The market is competitive and customers can easily switch providers, so developing customer loyalty is important
- Consultants and sales staff will need full access to IT resources from remote locations
- Customers will need access to the customer portal application but customer data should be segregated so that customers can access only their own data
- Customers expect high availability of the customer portal

Given this set of requirements, high-priority operations include:

- Acquiring devices and applications
- Proving service desk support
- Maintaining systems availability
- Developing applications
- Securing databases and hosts

A new business will of course need to acquire devices and applications, so managing that process well from the beginning is important. Also, as customer loyalty is so important in this market, service desk support will be a top priority as well. Supporting application development, system availability, and database and host security are the kinds of operations customers will not see directly but are fundamental to delivering services that are at the front lines of the business.

Post-Merger Organization

When two organizations merge, there are often plenty of technical issues to resolve. Integrating network architectures, databases, and applications requires knowledge of low-level details and careful planning. Once the systems are integrated, systems managers will have to apply management procedures consistently across all devices regardless of how they were managed in the past. In this scenario, some of the most important operations are:

- Asset management
- Service desk support
- Databases and host security
- Policy enforcement
- Improved quality controls on IT procedures
- Configuration management

One of the first challenges to address in a post-merger situation is compiling an accurate inventory. You cannot manage a device if you do not know you have it or if you do not know where it is or what kinds of applications are running on it. Asset management is one of the top few priorities in a post-merger environment.

Mergers can be disruptive to existing operations, so service desk support can be critical to maintaining operations and efficiency. Disruptions and changes in network architecture can introduce new and unforeseen security vulnerabilities. There is also the chance that existing patch management operations are disrupted during a merger that in turn perpetuate existing vulnerabilities. Another key area is to ensure policies are enforced and procedures continue to be carried out across newly acquired assets. The priorities in organizations going through less-disruptive changes are somewhat different.

Highly Regulated Organization

Highly regulated organizations, by definition, are subject to an array of compliance requirements. Typically, regulations require that organizations establish and follow certain policies and procedures as well as be able to demonstrate that these policies and procedures are in force. Simply put, they not only have to comply but must be able to prove they comply. For these reasons, some of the top priority areas for such an organization are:

- Asset management
- Systems monitoring
- Auditing and compliance reporting
- Databases and host security
- Policy enforcement
- Improved quality controls on IT procedures

Asset management is a fundamental service that enables several others. Having detailed information about the location, configuration, and status of all devices in the organization is the basis for reporting on them and demonstrating that they are in compliance. Asset management covers the full life cycle of hardware management, from procurement to disposal. Monitoring systems is another part of maintaining compliance because it is an early warning procedure that can help detect and control security breaches as well as other problems that can disrupt operations.

Auditing and compliance reporting are obviously necessary in this situation. Auditing involves more than the annual review by external auditors. Continuous monitoring and auditing of key events, such as failed access attempts, changes to deployed code, and configuration modifications should be logged and reviewed regularly.

Some of the most high-profile security breaches have involved the theft of information from databases. Part of database security is maintained with the database system itself, but much of that depends upon a secure host. Systems managers play a key role in securing databases by hardening host OSs and regularly monitoring the device for signs of security problems.

Establishing polices that meet auditor expectations can be challenging enough but ensuring those policies are enforced at all times in all applicable cases brings its own host of difficulties. Policies, for example, are platform neutral and must be enforced regardless of the device performing an operation. Consider the process of accessing a customer financial record; this could occur from:

- A desktop PC used by a customer support representative
- A batch process that runs from a central server updating account information on a regular basis
- A notebook used by an analyst investigating a problem with the account
- A smartphone, which combines cell phone and PDA functionality, used by the customer to transfer funds between accounts while traveling

Effective policy enforcement requires a combination of thorough planning and automation to ensure that all use cases are accommodated. This relates to the final high-priority need, improving quality controls on IT procedures. Monitoring operations is necessary but it may disclose weaknesses in some areas. For this reason, it is important to be able to measure the performance of IT operations, especially as it relates to compliance-oriented policies and procedures. Management reporting on operational procedures can help isolate problem areas and measure the effectiveness of various remediation plans so that procedures eventually meet expectations.

There is no absolute ordering of priorities that applies equally well to all organizations. Priorities will largely be driven by the business strategies of the organization (which are assessed in the first step of the roadmap process) and the current state of the organization. Although the priorities will vary, two themes are common across organizations making the move to service-oriented management: the need for a centralized repository of information and reporting and the benefits of optimizing policies and procedures.

Building a Central Management Foundation

Most, if not all, tasks associated with service-oriented management require or are made more efficient with the use of a CMDB, and some in particular, are virtually impossible without it:

- Change management
- Incident management
- Patch management

All these operations depend upon knowing what assets are in the organization, how they are configured, and how they relate to one another. A centralized repository provides information about individual assets as well as relationships between assets to delivered and agreed upon services. Gathering, verifying, and maintaining this can be a significant undertaking.

> 🕮 Creating and maintaining a CMDB is a well-established systems management practice. It is a central element of the ITIL framework; for more information about ITIL see, http://www.itil.co.uk/.

Types of Information in Centralized Repository

Building a centralized repository of information in a CMDB is best done in stages. First, the sections of the IT infrastructure should be prioritized and the most important configuration items addressed. This may include:

- Mission-critical servers
- PCs used in front-line support
- Key network devices
- In some cases, lines of business and other organizational structures

For each of these, the following information should be collected:

- OS running on the device
- OS version and patch status
- Applications on the device
- Location within the logical network
- Status of required software, such as anti-malware and host-based firewalls
- Network information, such as IP address and DNS server

In addition, relationships between devices should also be collected. This can include dependencies, such as:

- Devices dependent on particular routers and switches
- IP devices dependent on particular DNS servers
- Content filters and intrusion prevention systems (IPSs) assigned to particular subnets
- Outputs from one organizational unit as inputs to another unit

With a sense of the types of information to collect, the next challenge is how to collect it.

Methods for Collecting and Verifying Configuration Item Data

The level of information that should be tracked with configuration items is detailed enough and some of it changes frequently enough that automated methods are required to collect and maintain it. Two basic approaches are available: agent-based and agentless collection.

Agent-based collection depends upon a typically small program resident on devices that collect local information and update the configuration database. Although agents can be carefully designed to accommodate the specifics of each OS, this does introduce some management overhead. For example, the agents much be distributed, installed, and updated just like other applications on the devices. Furthermore, some systems managers might not want another piece of code running on devices that could in any way interfere with existing applications.

An alternative method is agentless data collection. With agentless information gathering, devices on the network are queried from a central server and no additional software is required on the device. This approach has several advantages, including:

- No software is required to remain resident on the client
- New devices can be detected without installing agents on the device
- Collection procedures are centrally managed

With a CMDB in place, an organization is just about ready to begin implementing service-oriented management practices. There is, however, one other area that must be attended to—optimizing policies and procedures.

Optimizing Policies and Procedures

Automation and centralized management of information can help streamline operations and make them more efficient; however, doing so cannot optimize operations to provide the greatest benefit to the organization. Consider an example. A hypothetical company has an ad-hoc approach to management and addresses basic tasks in the following ways:

- When new employees join the company, a notebook is ordered for the new worker unless one is readily available, perhaps from someone who just left the company. There is no central tracking of assets, so finding an existing asset depends on the memory of individual managers.
- When a vendor announces a patch, the systems managers decide at that time to install it or not, sometimes testing on non-production systems first and sometimes not. Without a prioritized ranking of assets, there is no way to quickly determine all the devices that should get the patch and in what order.
- Frontline IT support occasionally makes the rounds to check the status of anti-malware on notebooks. Most of the sales staff spend most of their time out of the office, so finding time to check their devices is a challenge. There is no single system for tracking which devices have been checked and which have not.

In such as extreme case as the one just described, one could install a CMDB, collect information about configuration items, and even keep it up to date with regular refreshes. The problem is it would do some good but not as much as possible. Potential benefits include:

- A single reporting system for which applications and OSs are running on each device
- A single reporting system for determining the patch level of each device
- A rudimentary asset-tracking system that could at least catalog basic information about devices on the network

What this approach would miss are the benefits that come from a combination of well-formulated management policies and automated services:

- Prioritizing devices in terms of mission-critical functions
- Linking documentation to configuration items
- Integrating asset management information with other management tools, such as patch management and deployment systems
- Enforcing policies based on attributes of devices and their users

Optimizing policies and procedures requires:

- An understanding of business goals and strategies
- Overall risk tolerance of the organization
- Regulations and other constraints on the organization
- An understanding of the existing IT infrastructure and plans for future changes
- A commitment to follow established procedures when carrying out IT management tasks

The last bullet point is one of the most important. The specific details of how one manages patches, deployments, or testing is often less important than the fact that one is following an established set of procedures. This is the topic addressed in the final step of the roadmap.

Roadmap Step 3: Implementing a Service Model for Systems Management

In many ways, the most difficult work is done by the time you reach the final step of the roadmap. Prior to this step, many of the issues have dealt with organizational readiness and the ability to adopt formal management procedures. The foundation has been set with the introduction of a CMDB and the tuning of policies and procedures. The next step is to put the product of these efforts into day-to-day management. For that, there are three factors to keep in mind:

- Adapting best practices
- Measuring operations
- Adapting to changing business requirements

Each of these high-level directives can help ensure the greatest benefit is derived from adopting a service-oriented management approach.

Adapting Best Practices

Best practices, like ITIL and COBIT, are complementary frameworks for understanding the kinds of tasks that must be performed to effectively manage and govern an IT operation. As anyone who has been in IT for a decade or more knows, best practices are like fashions: sometimes they are “in” and sometimes they are “out” but if you wait long enough, they will be back.

There is some logic to this cycle. Any best practice will address some of the needs of management. There are limits, though. Any best practice, such as ITIL, will not cover every conceivable issue facing an IT manager. For example, ITIL does not adequately address measuring management functions. Even if you completely implement ITIL practices, there will be other tasks that need attention. Some will see this as a flaw in ITIL and advocate some other set of best practices that are stronger on measurement. It is highly likely, though, that the new framework will be weak in some other area. The point is that no best practice framework will address all of a manager’s needs.

One way to benefit from a best practice frameworks is to use what they have, applying the ideas incrementally and in combination with other frameworks to find the most appropriate solution for your organization. Best practices do not manage for you; they do not alleviate the need to experiment and formulate your own solutions. They are excellent starting points, not final destinations.

Though out this guide, the discussion of service-oriented management has built on several best practices and frameworks, including:

- ITIL for infrastructure management
- COBIT for governance
- ISO-17799 for security

These will surely evolve and improve but are also sufficiently useful for immediate adoption.

COBIT and ITIL: Complementary not Competitive

COBIT and ITIL are both popular frameworks for managing IT, but they address different levels of management. They are best seen as complementing each other, not competing with each other.

COBIT is a governance framework. The goals of COBIT are to align IT operations with business objectives and to ensure successful implementation of those objectives. COBIT is divided into four main areas:

- Planning and organizing
- Acquiring and deploying
- Delivering and supporting
- Monitoring and evaluating

These cover the full breadth of IT operations. ITIL, however, is more focused on delivery of services and support, assuming proper alignment and governance are already in place. The core areas of ITIL are:

- Service support
- Service delivery
- Planning service management
- Security management
- Infrastructure management
- Application and software asset management

Both COBIT and ITIL can be implemented independently but the high-level executive perspective of COBIT also works well alongside the procedural management perspective of ITIL.

Another framework that is commonly used is the COSO framework (from Committee of Sponsoring Organizations of the Treadway Commission), which primarily addresses financial governance and management. This best practice addresses several areas, including:

- Internal control environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

The objective of this framework is to identify the processes and executive management tasks associated with the rational pursuit of organizational objectives, the efficient use of resources, and proper and responsible reporting to stakeholders. COSO addresses broad organizational functions, not just IT operations, but it is often discussed, along with COBIT, as a means of achieving compliance with government regulations, particularly SOX.

Measuring Operations

There is an old saying that you cannot manage what you do not measure. This is certainly true in IT. One does not need to measure every aspect of every procedure and operation. Rather, it is better to find representative measures for key services, such as:

- In service support, the number of service desk calls, the duration of calls, and the number of calls escalated
- In patch management, the number of patches applied, the number of failed patch operations, and the time required to apply patches
- In deployment management, the number of devices updated, the number of failed deployment attempts, and the staff hours required
- In change management, the number of changes, the time to approve changes, and the number of emergency changes

Like best-practice frameworks, these examples are starting points for formulating sets of measures that reflect the state of IT infrastructure and operations.

Adapting to Changing Business Requirements

Business requirements are dynamic. Sound IT management practices are relatively well structured but still accommodate change. The goal for IT management is to provide a stable infrastructure that can be applied in different ways and can be changed relatively easily. Several factors contribute to this:

- Use of management best practices—There is no re-inventing of the wheel
- Use of standardized architecture—Variations and exceptions increase management challenges
- Commitment to policies and procedures—Every exception to these creates potentially more work for systems administrators at later times
- Centralized repository of configuration data so that information is available when needed

Service-oriented management as described throughout this guide contributes to the adaptability of an organization and, when used in conjunction with best practices such as ITIL and COBIT, provides the foundation for an adaptable IT organization.

Summary

Management models that have worked in the past in more slowly changing business environments are no longer sufficient for the dynamics of today's IT operations. To enable an adaptable operation, you must assess the current status of IT operation, if necessary, plan a transition to a mature service model based on frameworks such as service-oriented management, ITIL, and COBIT, and finally implement and maintain the practices outlined there. IT management is demanding but the tools and practices are established to help you bring direct value to organization.

Throughout this guide, service-oriented management has been presented as a means to address the key challenges facing IT operations, including:

- Business objectives and IT alignment
- Planning and risk management
- Business continuity and operational integrity
- Security and compliance
- Capacity planning
- Asset management
- Service delivery

The key features of a service-oriented management strategy that serve this goal include:

- Modularity of services
- Comprehensive management of configuration items in a centralized repository—the CMDB
- Ability to report on assets and dependencies between assets
- Support for maintaining adequate security in the information infrastructure
- Support for asset management
- Support for the delivery of new IT services and applications

There is no single process or methodology that will guarantee the success of an IT operation. There are, however, well-developed best practices that provide ideal starting points and detailed guidance on managing a significant part of any information management operation. That in conjunction with the ability to adapt to the particular needs of your own organization is the best approach to meeting your organization's long-term goals and objectives.

Download Additional eBooks from Realtime Nexus!