



realtimepublishers.com[®]

The Definitive Guide[™] To

Service-Oriented Systems Management



altiris[®]

Dan Sullivan

Chapter 3: Industry Standard Practices and Service-Oriented Management.....	47
Organizing IT Operations Around SOM	48
Overview of Best Practice Frameworks	49
Best Practice Principal 1: IT Services Have Much in Common.....	49
Best Practice Principal 2: IT Services Are Interdependent.....	50
Best Practice Principal 3: Measure IT Services.....	50
KPIs.....	51
Best Practice Principal 4: Utilize Repeatable Process	55
Best Practice Principal 5: Leverage Broadly Applicable Models.....	56
Frameworks and SOM	56
Best Practice Frameworks and SOM	57
Technology Management and ITIL	58
Service Delivery within ITIL.....	58
Service Support within ITIL	59
Planning to Implement Service Management	60
Security Management	60
Infrastructure Management.....	60
Release Management	60
Other ITIL Disciplines.....	61
COBIT.....	61
Planning and Acquiring	62
Acquiring and Implementing	62
Delivering and Supporting.....	63
Monitoring and Evaluating	63
Information Security and ISO 17799.....	64
Risk Management and NIST Guide for Technology Systems.....	65
Risk Mitigation	66
Risk Evaluation and Assessment	67
Leveraging SOM to Support Frameworks and Standards	67
Summary	68

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>.]

Chapter 3: Industry Standard Practices and Service-Oriented Management

Civilizations advance by preserving, passing on, and building upon existing knowledge. If we had not leveraged the advances of previous generations, our world would be a far different place. In a similar fashion, although on a far less expansive scale, IT practitioners have developed, formalized, and documented best practices in several areas related to managing IT services, particularly in the following arenas:

- Technology management
- Governance
- Security
- Risk management

Starting with best practices saves us from “reinventing the wheel” with commonly required procedures and methodologies. Many of us would never think of building computers from scratch when we can buy them off the shelf, perhaps with some customization. In the same way, we can take a number of best practices and adapt them to our organizational requirements without reasoning from first principals to determine the best way to accommodate change, plan for capital spending, secure the infrastructure, and a host of other tasks demanded of IT managers and systems administrators.

This chapter will begin with a brief discussion of the need for organizational frameworks and standards. It then provides an overview of four broadly applicable standards:

- IT Infrastructure Library (ITIL)
- Control Objectives for Information and related Technology (COBIT)
- ISO 17799 security standards
- National Institute of Standards (NIST) Guide for Technology Systems related to risk management

The chapter concludes with a discussion on the contribution these frameworks make to the practice of service-oriented management (SOM) practices.

Organizing IT Operations Around SOM

The skills required to manage IT services are a mosaic of technical, business, and organizational talents that can take years to acquire, develop, and hone. Some can be taught; some we learn the hard way. Regardless of how one learns how to manage IT services, to successfully control and protect complex IT operations, we have to know a few things:

- First, what factors within IT service operations need to be managed?
- Second, what controls must be in place to ensure those factors are managed?
- Third, how do you balance competing needs, such as the need for accessible yet secure systems?

One of the first steps to getting a handle on the complexity of managing IT services is to organize the constituent processes of IT operations into a comprehensive model. Although there are many ways to organize the constituent processes, the one that is used in this guide is SOM.

Within the SOM model, IT operations are divided into several distinct services:

- Network management
- Server and application management
- Client management
- Incident response
- Change control
- Monitoring and event management
- Asset management
- Application development


These divisions will appear familiar to many in IT because organizations often structure their IT departments along similar lines. For example, large organizations often employ distinct groups that manage the network, servers, and client hardware. There are also cross-functional teams to address issues that span the organizational structure. For example, change management and incident response will require expertise in all areas of IT, not just a single one.

In addition to following common organizational structures, the SOM model fits well with best practice frameworks in use within IT. ITIL and COBIT address the breadth of topics covered by SOM. Other more specialized frameworks—such as ISO 17799 security standards and the NIST Guide for Technology Systems related to risk management—provide a focused set of best practices for subdivisions of IT operations.

When organizing IT operations around the SOM model, it makes sense to leverage best practices that fit with that model. The next section will examine common characteristics of several IT management frameworks; this will be followed by discussions of the individual frameworks.

Overview of Best Practice Frameworks

As discussed in Chapter 1, there are various approaches for determining what works and what does not work in information management. Three approaches were identified: ad hoc systems management, controlled systems management, and continuously improving systems management. In theory, one could start from scratch with controlled systems management and continuously improving systems management. (In practice, ad hoc approaches to system management always start from scratch). A better approach is to build on what has already been developed.

 For more information about the three IT management methods, see Chapter 1.

You can take much from what others have learned if you keep in mind several principals about the use of best practices as they apply to SOM:

- IT services have much in common
- IT services are interdependent
- IT services can and should be measured
- IT services are repeatable processes
- IT services are broadly applicable

These principals speak to management of IT services within as well as across organizations. They are also embodied in the four frameworks described in the following sections.

Best Practice Principal 1: IT Services Have Much in Common

No matter how different your business or organization may be from others, it surely also has much in common with them. Whether an IT group is supporting a startup professional services business, a long-established manufacturer, or a government agency, there are IT requirements common to all:

- The need to define, procure, and manage hardware and software
- The need to manage changes to infrastructure and applications
- The need to maintain a secure and dependable environment
- The need to plan for future needs
- The need to manage the financial aspects, including risks, of IT operations

None of these requirements change depending on the type of operating system (OS) run on your servers, the volume of data pushed through your network, or the kinds of applications used by your employees.

Best Practice Principal 2: IT Services Are Interdependent

Large IT organizations are often divided into specialized groups: one group supports network operations, another manages database administration, a third group supports desktop applications, and still another group is responsible for software development. This division of labor is essential to having the depth of knowledge required to master the different disciplines within IT.

For example, a network administrator might spend a fair amount of time learning a network monitoring tool that allows the administrator to analyze traffic at the packet level. A database administrator is the person that understands the details of database listeners that support communications between database instances and client applications. A desktop support specialist may be the first point of contact for an employee with a problematic application. So, when a user gets a message that his or her applications cannot connect to the database, who is responsible? They all are.

The desktop support specialist can probably quickly isolate the problem as having to do with the application configuration, a network problem, or an issue with the database server. If the configuration files and registry settings appear correct and basic connectivity with the database server is available, it may be time to call the database administrator.

The database administrator, in turn, can verify whether the necessary database processes are running, the user has proper authorization on the database application, and the proper protocols are configured on both the client and the server. If the database seems to be functioning properly and the client still cannot connect, it is time to dig deeper and bring in the network manager.

At this point, the network manager might want to monitor traffic between the client and the database. Are all the protocols that should be running actually in use? Are there any problems with firewalls or routers between the client and the server? Together, an application support specialist, a database administrator, and a network manager can diagnose problems that span multiple domains more effectively than if they worked in isolation. Coordinating among different areas is a crucial factor in the successful delivery of IT services.

Best Practice Principal 3: Measure IT Services

Regardless of the type of IT service being provided—whether it is network bandwidth or financial and project management services—the service can and should be measured.

Measurements have several characteristics:

- Key performance indicators (KPIs)
- Baselines
- Trends

KPIs

KPIs are events or attributes that are measurable and correspond to the level of service delivered. There are several types of KPIs with varying characteristics:

- Technical
- Financial
- Organizational

Best practices for a particular area might include more of some of these than others, but the most comprehensive best practices address all the main types.

Technical KPIs

Some KPIs are easily identified, especially technical ones, such as megabytes of data transmitted over a network segment in a given period of time, the latency on a network, the storage utilized on a disk array, and the percent of available CPU time utilized for application processing. By their very nature, technical KPIs are easily quantified. They are also easily gathered, relatively speaking. Applications, OSs, and dedicated appliances can generate large amounts of data about performance and capacity.

The ease with which data on technical measures is generated is both an advantage and a disadvantage; information overload is a constant problem when managing with technical elements of IT services. Thus, the goal of measuring IT services is not to measure all services or every dimension of an operation but to focus on a small number of key measures that are indicative of the overall performance of the service.

As Figure 3.1 shows, even simple operations, such as measuring CPU and disk activity, can generate too much data to allow for quick assessments of the state of an operation. KPIs for server performance might include:

- Percent of non-idle CPU time
- Disk reads and writes per second
- Total bytes received and sent per second from a network interface
- Number of page faults per second

This set of measurements provides one measure per major functional area of a server (CPU, disk, network, and memory) and can be monitored nearly continuously or polled at longer intervals with the data aggregated to provide a performance measure for a specific period of time.

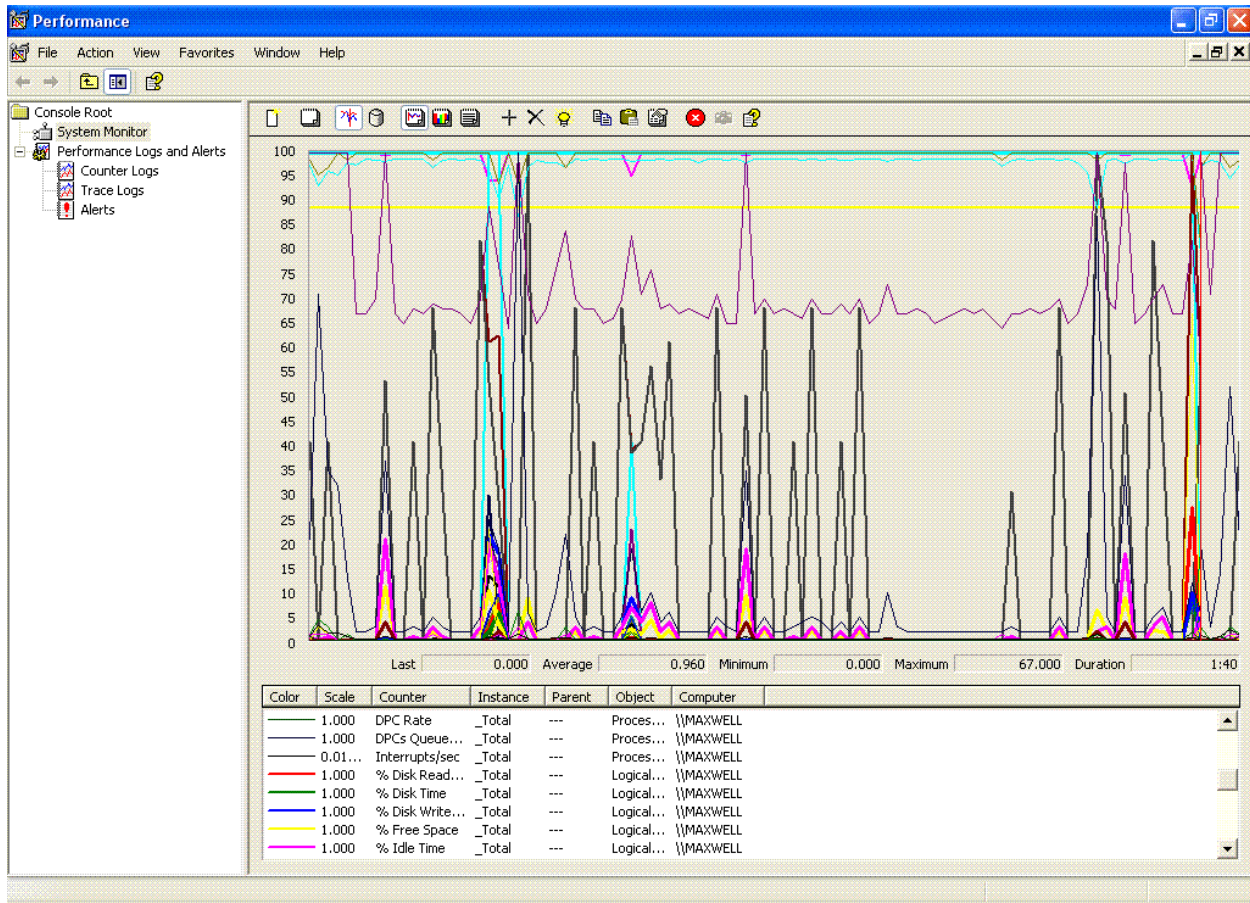



Figure 3.1: Information overload is a common problem when measuring technical performance.

As important as technical measures are, they do not provide a complete picture of the state of IT operations. Financial measures are another critical component of IT operations management.

Financial KPIs

Financial KPIs allow managers to assess the value of specific IT operations and services relative to their costs. Unlike technical measures, financial measures do not tend to lend themselves to the massive amount of data found with machine-generated measures.

Financial measures tend to focus on the cost of labor and equipment, the return on investment (ROI) of proposed purchases, and financial management issues, such as budgeting and cash flow. These tasks are well understood and documented elsewhere; the focus here is on topics that are too often overlooked or under-addressed in textbook discussions of IT management.

 For information about other aspects of IT financial management, see resources such as ComputerWorld's IT Management Knowledge Center at <http://www.computerworld.com/managementtopics/management>, and CIO Magazine's CIO Resource Center at <http://www.cio.com/leadership/itvalue/>.

When formulating financial measures, be sure to understand the scope of the measure. For example, the “cost” of a server may be stated as \$20,000, when in fact that is the cost to purchase the server from the vendor. The full cost of introducing that server into the organization would have to include at least the vendor invoice amount, plus:

- Labor costs to install and configure the server and its OS
- Staff time dedicated to change management operations, including plan review for the server
- Information security staff time spent locking down the server and auditing it as needed
- Compliance management staff time spent understanding implications of the use of the server—for example, will confidential financial information be stored on the server?
- Network services support time spent updating routers, firewall, intrusion prevention systems (IPSs), and other services that must be aware of the presence of new devices
- Server support staff time required to add the server to the backup and disaster recovery process
- Application support time required to install and configure packaged or custom applications running on the server
- Additional software licenses incurred because of the new server

Accurate financial measures are often difficult to formulate and, in reality, we often settle for estimates. In addition to understanding the breadth of costs related to IT, it is important to avoid unintentionally equivocating about the meaning of terms.

Related to identifying the scope of terms appropriately, you also must use terms precisely. Too often within an organization, a single term will take on multiple meanings, depending on the context. For example, to the sales department, the cost of goods sold may include the price paid for a good, shipping costs, and storage and inventory management costs; the finance department may include all those factors as well as the sales commission paid to the salesperson that made the sale. It is not the case that one group is wrong and another is right. The problem lies in multiple uses of the same term. Using multiple terms, such as pre-sales cost of goods sold and post-sales costs of good sold can help avoid this confusion. As difficult as financial measures are to formulate precisely, they are not as challenging as organizational KPIs.

Organizational KPIs

Organizational KPIs are soft measures; they do not have obvious quantifiable aspects, as technical and financial measures do. Technical measures are relatively easy to grasp. The problem with them tends to be too much information. In the case of financial measures, you must define terms precisely and with appropriate scope to accurately reflect the costs and benefits of investments. Just defining organizational KPIs is difficult. Some of the areas that are included in organizational KPIs are:

- Training level of staff
- Ability to incorporate emerging technologies into existing infrastructure
- Ability to execute new organizational models, such as partnering and outsourcing
- Ability of IT to meet needs and expectations of business units
- Level of overall compliance with government regulations

Although difficult to quantify, organizational measures reflect the ability of an organization to execute strategies and perform operations.

Another aspect of these different types of KPIs is that they are not independent of each other. The ability to effectively provide key technical services depends upon the ability to fund the staff and equipment needed; having a well-trained staff that understands change management procedures and executes them appropriately is an organizational KPI that has direct impact on technical operations.

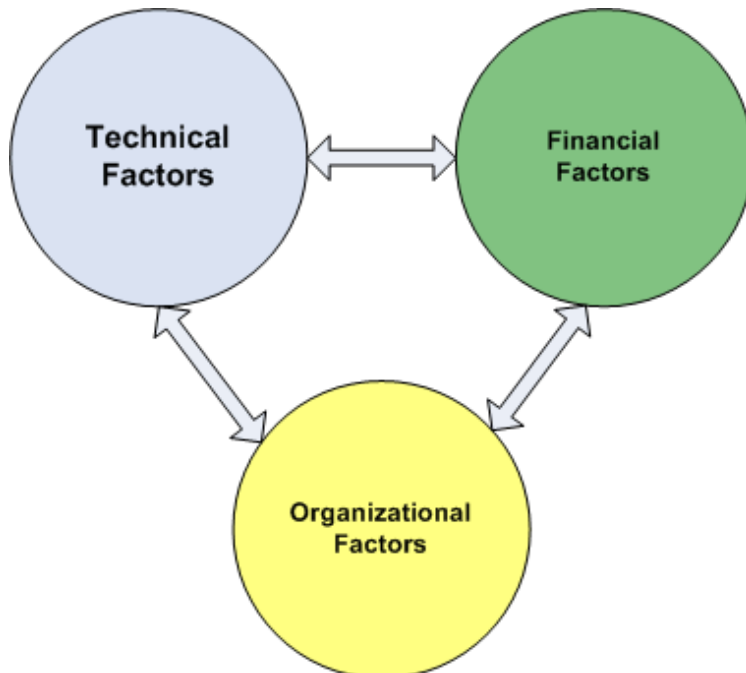



Figure 3.2: The three types of factors that are measured by KPIs interact and influence each other.

Measurement is a key process in SOM, particularly in the frameworks and best practices that support it. Another characteristic of these best practices is the ability to leverage repeatable processes.

Best Practice Principal 4: Utilize Repeatable Process

Processes, as an object of organizational study, have received quite a bit of press in the last decade. “Business process reengineering” was one of the techniques advocated by leaders in organizational management and corporate strategy as a way to shift corporations away from internally directed behaviors to more customer-focused activities that leverage information technologies. Reengineering entered the IT lexicon primarily as a process that other parts of the organization, especially front-line business units, had to understand, implement, and manage. IT was playing a supporting role in the beginning, but that has changed.

 For more information about organizational reengineering, see Michael Porter’s *Competitive Advantage: Creating and Sustaining Superior Performance* (New York: The Free Press, 1985), Peter Drucker’s “The Coming of the New Organization” (Harvard Business Review, Jan-Feb. 1988), and M. Hammer and S.A. Stanton’s *The Reengineering Revolution: A Handbook* (New York, Harper Business, 1995).

Process reengineering has had its counterpart in IT with the widespread adoption of standard process management policies and procedures. The goal is typically to improve consistency and quality of services while controlling costs. Many of the frameworks described in this chapter emphasize specific processes, including service level management, change management, disaster recovery, capacity planning, security management, and a host of other essential IT services.

The focus on processes within IT has been driven by several advantages provided by their adoption:

- Ability to deliver consistent and predictable performance—For example, with simple tasks such as adding users access rights to an application to more complex processes, such as incident response
- Ability to measure performance and compare results—With consistent, repeatable processes, KPIs can be identified and measured
- Ability to improve procedures—Again, with consistent procedures, organizations can measure performance, analyze performance data, and identify weak areas in those processes
- Ability to justify budgetary needs—With hard numbers on system capacity and trends in growth of users and applications, IT managers can more effectively defend their requests for appropriate funding

Processes are common to virtually all IT operations, so it is not surprising to find them prominently in best practice frameworks, especially those so closely associated with SOM practices. This fact highlights another aspect of these frameworks—that is, they leverage broadly applicable models across industries.

Best Practice Principal 5: Leverage Broadly Applicable Models

The practices of SOM and related frameworks are not specific to any one industry. Certainly, some areas of a framework may receive more emphasis in some industries than others.

For example, the role of business continuity will have a high priority in financial services and healthcare operations; consulting businesses, although concerned with business continuity, are less prone to centralized business disruptions because of the distributed nature of their operations. Similarly, government agencies managing sensitive information will implement security measures most of us would consider cumbersome and unnecessary for routine business operations.

SOM is not an industry-specific model but a general model for understanding and managing core IT services. It also recognizes the shared goals found in many IT organizations:

- Improved visibility and control of operations
- A standardized IT infrastructure and supporting services
- Improved automation and quality control
- Improved security
- Attaining and remaining in compliance with government regulations

SOM recognizes that the common goals of IT operations and best practice frameworks provide guidance on policies, procedures, and processes needed to attain those goals.

Frameworks and SOM

Although SOM defines what should be done in IT management, the best practice frameworks described in this chapter provide information about how to effectively implement a SOM approach. As Table 3.1 shows, each of the best practice frameworks has much to offer in the way of SOM guidance.

Although there is much overlap—for example, all the frameworks have something to say about network management—some frameworks provide more detail than others: COBIT addresses incident response, but ISO 17799, with its focus on security, has much more to say about this critical area of information security management.

Service Oriented Management Area	Best Practice Framework			
	ITIL	COBIT	ISO 17799	NIST Guide for Technology Systems
Network management	X	X	X	X
Server and application management	X	X	X	
Client management	X	X	X	
Incident response	X	X		
Change control	X	X		
Monitoring and event management	X	X	X	X
Asset management	X	X	X	X
Application development	X	X	X	

Table 3.1: Best practice frameworks address multiple areas of SOM.

The following section will examine the particulars of each of these best practice frameworks.

Best Practice Frameworks and SOM

There are many best practice guidelines and frameworks within IT. Many are focused on narrow aspects of systems management, application development, or a particular type of operation. Although useful in some situations, those frameworks will not be addressed in this section, which focuses on broadly applicable guidelines:

- ITIL
- COBIT
- ISO 17799 security standards
- NIST Guide for Technology Systems related to risk management


ITIL is particularly relevant to technology management. COBIT is as well but also addresses many essential aspects of governance and compliance. ISO 17799 is more narrowly focused on security, but that topic is so wide-ranging that it warrants inclusion in this set of broad frameworks. Finally, the NIST Guide for Technology Systems addresses risk management, which, like security, spans all other IT management operations.

Technology Management and ITIL

ITIL was defined under the auspices of the Office of Government Commerce within the British government. The practices defined within ITIL have been codified within the ISO standard, ISO 20000. ITIL defines several disciplines within IT management:

- Service delivery
- Service support
- Planning to implement service management
- Security management
- Infrastructure management
- Business perspective
- Application management

Two disciplines, service delivery and service support, are perhaps the most widely used of the disciplines.

 ITIL is an open standard, so it can be freely adopted by organizations. The content of the ITIL references is copyright protected, however. To purchase ITIL framework books, see <https://securewsch01.websitecomplete.com/itil-survival/shop/showDept.asp?dept=17>. Community support is available at <http://www.15000.net/>.

Service Delivery within ITIL

Service delivery topics within ITIL focus on elements of IT processes that are needed to ensure services are available and meet the needs of IT customers. Service level agreements (SLAs) play a central role in service delivery. They constitute the set of requirements that IT must meet. SLAs depend upon adequate measurements (discussed earlier) to determine whether agreements are met. These measurements are also used to assess the consequences of changes in the IT environment to the quality and level of service. For example, if the network services group has an SLA to provide a set level of network bandwidth availability to one business unit, it cannot then enter into an agreement to provide additional bandwidth to another business unit without first determining the impact on the first customer.

Similarly, service delivery must address capacity planning. Capacity of resources spans computational resources, network resources, storage services, and applications provided. Measuring current utilization as well as planning for future needs are both part of capacity planning.

Continuity management and availability management are also elements of service delivery. The focus of these areas is the ability to continue to provide IT services in the event of a business disruption, such as a natural disaster. This entails planning, monitoring, testing, and execution of business continuity plans.

The final element of service delivery addressed in ITIL is financial management with an emphasis on understanding the total cost of ownership (TCO) of IT resources. As described earlier in the section on financial KPIs, comprehensive measures, which take into account all costs, is fundamental to financial management.

Although service delivery tends to address longer-term planning challenges in IT, the service support discipline of ITIL concentrates on shorter-term needs and issues.

Service Support within ITIL


Within the ITIL framework, a single point of contact is provided for end users. This point of contact, commonly called a service desk, coordinates multiple activities for users:


- Help desk support
- Problem escalation
- Change management
- Status reporting

The benefit of integrated service support for end users is the single point of contact for all IT-related issues. In addition, this support helps IT professionals through the service desk's broad perspective. For example, if a user calls with an application problem, the service desk contact would have information about recent changes to application servers, reports on network performance, and information about other events within the IT environment that could impact the user's application.

Contrast that with typical Help desk interactions in which users are asked for their user IDs, application names and versions, and a host of other information that should be readily available to the support personnel. Help desk support often have limited access to information about the current state of operations and have to depend on libraries of past incidents to help solve problems based on those incidents.

Service support within ITIL shifts the focus from narrowly defined Help desk-like problem resolution to a more comprehensive approach to customer support.

 This shift from a narrow, problem-centric approach to a more comprehensive view only works when service support staff has comprehensive information. A central aspect of SOM is the use of a centralized repository of information in the form of the configuration management database (CMDB). Without a CMDB or similar database, service support reverts to a less-effective silo-based problem management practice.

 Chapter 4 will provide details about CMDBs and their role in SOM.


A centralized approach to information sharing supports other areas of service support, including problem management, configuration management, change management, and release management.

Planning to Implement Service Management

The third discipline with ITIL, planning to implement service management, addresses business alignment. This topic examines the need to:

- Understand the strategic plan of the organization, and IT's role within that strategic plan
- Assess the current state of IT services
- Establish objectives for meeting strategic needs
- Implementing the processes, policies, and procedures
- Measuring performance relative to objectives

Again, the topics addressed within ITIL dovetail well with SOM, which is driven, in part, by fundamental business objectives, including business alignment.

 Chapter 1 includes a more detailed discussion of business alignment with a discussion of coherent business strategies, managing multiple objectives, and dynamic requirements.

Security Management

ITIL has adopted ISO 17799 as a basis for security management. That framework is discussed in more detail in a bit.

Infrastructure Management

ITIL's section on infrastructure management addresses four elements: design and planning, deployment, operations, and technical support. The design and planning part of infrastructure management spans business requirements to technical and architectural issues surrounding the development of IT infrastructure. Tasks include developing business cases for plans, conducting feasibility studies, and designing architectures. The deployment operations include project management and release management procedures to improve the likelihood of a successful rollout of new hardware and applications. Operations management addresses the day-to-day activities that keep an IT infrastructure operational. These include system monitoring, log review, job scheduling, backup and restore operations, and utilization monitoring. Technical support encompasses a number of services, including documentation, specialist support for problem resolution, and support for technical planning.

Release Management

Once software components have been acquired or developed, and tested in a quality assurance environment, they are ready for production release. Release management is the practice of moving software components into operation; this entails several steps, including:

- Adding software to a definitive software library
- Analyzing dependencies in the production environment and ensuring that the new software is configured to function properly
- Scheduling resources to install and configure software
- Coordinating with training, Help desk, and other support personnel

Release management is a bridge process that moves software from project to operational status.

Other ITIL Disciplines

Other disciplines in ITIL are equally linked to SOM operations. The business perspective discipline, for example, includes continuity planning and change management. It also extends beyond the scope of SOM to cover topics such as outsourcing. (Of course, outsourcing would have an impact on operations governed by SOM, but SOM does not address business structures, such as outsourcing, directly). Application management within ITIL discusses software development methods and practices. ITIL is a broadly adopted framework for IT management; another similar framework is COBIT.

COBIT

Governance has grown in importance along with increasing demands for compliance with government regulations. For publicly traded companies and government agencies in particular, ad hoc management procedures are no longer sufficient. Well-defined policies and practices that support specific objectives defined in regulations are demanded of IT professionals.


COBIT was developed by the Information Systems and Audit Control Association (ISACA) as a framework for controlling IT operations. Although there is less emphasis on execution than ITIL offers, much of COBIT can help improve operations. COBIT is well designed to support governance and complements ITIL's focus on operational processes.

COBIT is a process-centric framework with four broad subdivisions:

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

Like the disciplines in ITIL, these processes are common to IT operations regardless of size or industry. Within the COBIT framework, these processes are managed through a series of controls. Each control includes an objective that is to be achieved, a method for achieving it, and metrics for measuring the success of the control objective.

As the name implies, controls are in place to ensure objectives are met and processes can be improved. These controls help to define the operational tasks that must be performed to maintain compliance with both internal and external process requirements. Although COBIT is not designed for a particular regulation, the breadth and focus of the framework makes it well suited for meeting the demands of many regulations.

 For details on COBIT, see the ISACA Web site's COBIT offerings at <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>.

Planning and Acquiring

The planning and acquiring area of COBIT includes business and organizational-oriented control objectives. As noted earlier in this chapter in the discussion of KPIs, organizational objectives are sometimes difficult to quantify. COBIT accommodates that challenge by defining a set of high-level control objectives that are further refined into more quantifiable objectives. The key areas of planning and acquiring processes include:

- Defining a strategic plan and determining technical direction
- Defining an information architecture and the processes and organization that support it
- Managing IT investments
- Communicating aims and managing human resources
- Managing quality, risks, and projects

Within these areas of planning and acquiring, each control objective includes a set of goals, activities and metrics for measuring KPIs. Goals establish what is to be done, activities define how to accomplish those goals, and the metrics are used to understand the effectiveness of the activities. For example, within the objective of establishing a strategic IT plan, there are several activities, including identifying critical dependencies, documenting IT strategic plans, and building tactical plans.

These activities are measured with KPIs. Again, using the strategic planning process as an example, the KPIs include the delay between modifying business strategy and updating IT strategy, the percent of IT projects directly linked to IT tactical plans, and the degree of compliance with business and government regulations.

Acquiring and Implementing

Acquiring and implementing processes focus on bringing technology into the organization and enabling its use through proper change management and installation procedures. The key control objectives within this area include

- Identifying IT solutions and maintaining the associated software and hardware
- Ensuring documentation and training are available to enable the use of procured systems
- Managing the changes to infrastructure and operations
- Validating and accrediting the installation of new systems

COBIT defines procedures focused on controlling these processes to ensure that they follow established procedures. For example, before one can accurately identify needed software, one must define the business requirement for the application first. Similarly, to validate and accredit a hardware installation, the new system must be tested in an appropriately configured test environment.

Metrics in this area focus on the delivery of functional systems and include a number of emergency change requests, availability and accuracy of documentation, and percent of requirements met by acquired systems.

Delivering and Supporting

Delivering and supporting processes have the most control objectives of all COBIT activities. This is not surprising because delivering and supporting constitute the bulk of IT activities. The control objectives defined by COBIT for this activity include:

- Defining and managing service levels as well as managing outside service providers
- Ensuring continuous operations with appropriate levels of security and adequate capacity
- Providing technical support for users and configuration management for infrastructure
- Managing data as well as physical environment
- Managing day-to-day operations, such as job scheduling and output generation

The goals within this activity are similar to service areas discussed earlier in the ITIL section. They include capacity planning, system monitoring, defining security plans, and establishing and managing financial controls. Key metrics in delivery and support include percent of assets included in capacity planning operations, the frequency of business disruptions due to unavailable IT services, and the time between recognizing the need for training and the delivery of that training.

Monitoring and Evaluating

Monitoring and evaluating is the fourth activity area within COBIT. The focus of these activities is four closely related objectives:

- IT performance
- Internal control
- Compliance
- Governance


In each of these control objectives, the goal is to ensure that the service levels, standards, and other requirements on IT operations are actually met. Internal controls and compliance focus on ensuring IT activities meet audit requirements as well as government regulations. IT performance and governance objectives control the alignment of IT with business objectives and ensure that IT operations remain synchronized with the goals and objectives of the organization's leadership. Key metrics include the percent of critical processes that are actively monitored, the time between identifying a process deficiency and the time it is corrected, and the time between the issuance of a regulation and the time IT comes into compliance.

COBIT is a comprehensive framework that can be used with SOM models to implement controls over IT services. The focus of SOM is to identify key services and enable their efficient and effective management. COBIT is a framework that helps to meet that goal by defining thorough and detailed control objectives. COBIT is structured with a clear definition of goals, activities, and KPIs for the breadth of IT activities.

In addition to frameworks, such as ITIL and COBIT, that address the breadth of IT operations, other useful frameworks focus on targeted areas within IT. The ISO 17799 security standard is one such framework.

Information Security and ISO 17799

The ISO 17799 standard, also known as the Code of Practice for Information Security Management, is a set of control measures focused on preserving information security in a wide range of organizations. It includes several subdivisions, each of which is composed of a series of controls for preserving information security.

 For more information about ISO 17799, including training material, articles, and compliant policies, see the ISO 17799 Information Security Portal at <http://www.computersecuritynow.com/>. Two user-supported sites provide additional information—the ISO 17799 Guide at <http://iso-17799.safemode.org/> and the ISO 17799 Community Portal at <http://www.17799.com/>. The full standard can be purchased and downloaded from <http://17799.standardsdirect.org/>.

The main subdivisions are:

- Security policy
- Security organization
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

Security policy, security organization, and asset classification and control address the need for well-defined policies and procedures that protect the confidentiality and integrity of information and the availability of infrastructure. Personnel security addresses the need for user awareness training, and the physical and environmental security section covers the protection needs of physical assets and safeguards for ensuring their integrity. Communications and operations management deals with network security, and access control covers areas such as identity management, authentication, and authorization of users.

System development and maintenance focuses the security needs of software development, particularly those related to ensuring systems are developed with minimal risk of introducing vulnerabilities when the system is deployed.

Business continuity and compliance address the same areas as their counterparts in ITIL and COBIT—namely, ensuring that businesses will continue to operate despite disruptions and will operate in compliance with relevant regulations.

The parallels between ISO 17799 and SOM are obvious. SOM and ISO 17799 share a number of common areas, including network management, asset management, application development, and server and client management. Although SOM applies to other aspects of IT management in addition to security, the practices and information gathered during SOM operations are relevant to security management. Again, as with other best practices described in this chapter, ISO 17799 can help guide management processes to realize the greatest benefit from a SOM model.

Risk Management and NIST Guide for Technology Systems

The risk management guide published by the United States NIST is a set of best practices for protecting organizations from IT-related risks. As the guide clearly notes, “The risk management process should not be treated as primarily a technical function carried out by the IT experts who operate and manage IT systems, but as an essential management function of the organization” (“Risk Management Guide for Information Technology Systems,” NIST Special Publication 800-30, p. 1). This directive is derived from the same perspective common to all four best practice frameworks discussed in this chapter; that is, that IT operations and services must be aligned with business and business drivers must be IT drivers.

 The full Risk Management Guide for Information Technology Systems is freely available at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

While recognizing the need to align business and technical objectives of risk management, the guide defines three processes in risk management:

- Risk assessment
- Risk mitigation
- Evaluation and assessment

The first step, risk assessment, is comprised of seven steps:

- System characterization, which defines the scope of the risk management effort and identifies the assets and organizational units (OUs) involved in the effort.
- During threat assessment, threats, or potential agents of disruption, are identified along with their sources.
- Vulnerability assessment discovers weaknesses in existing infrastructure that leaves the system predisposed to disruption by threats.
- Control analysis, the fourth step, examines the controls, or countermeasures, in place or planned for deployment that mitigate the potential for disruption by threats.
- Likelihood determination tries to pin down the probability of disruption given a set of threats and vulnerabilities. This process takes into account motivation and capabilities of the potential perpetrators, the nature of system vulnerabilities, and the effectiveness of existing controls.
- Impact analysis determines the cost of disruptions caused by a threat being exercised against an organization.
- Risk determination takes into account the impact of a threat and the likelihood to determine the risk to the organization from that threat.

With the outcome of the risk determination phase, an organization can move to the next stage, risk mitigation.

Risk Mitigation

During the risk mitigation phase, information learned in the risk assessment phase is used to determine appropriate measures for reducing risk for the least cost and with the least disruptive impact on the organization. The risk mitigation phase has several components:

- Understanding risk mitigation options
- Developing and implementing risk mitigation strategy
- Conducting cost benefit analysis and dealing with residual risk

There are several risk mitigation options outlined in the NIST guide:

- Risk assumption, which essentially accepts the risks or provides for some controls to reduce the risk
- Risk avoidance, which requires steps to remove the cause of the risk
- Risk limitation, which lessens the impact of a risk by use of preventive controls
- Risk planning, which introduces prioritized controls
- Research, which entails investigating the risk in an effort to discover new controls
- Risk transfer, which entails purchasing insurance to transfer the risk to a third-party

The guide provides several rules of thumb for risk mitigation strategies. First, if a risk does exist, try to reduce the likelihood the vulnerability will be exercised by applying layered protection and other architectural devices and administrative controls. Second, increase the cost to the potential perpetrator so that the cost exceeds the value of the information stolen. Finally, when the cost is great, purchase insurance to mitigate risk.

The risk mitigation strategy is implemented through a series of technical, management, and operational controls. Technical controls contain some element of hardware, software, or architectural countermeasure to mitigate risks. Management controls focus on policies, procedures, and guidelines that work in conjunction with other types of controls to mitigate risks. Operational controls focus on the governance of security measures and the identification of weaknesses in the existing security posture of an organization.

Cost benefit analysis studies help to identify the set of controls in place, their cost, and their impact on reducing risk. The purpose of conducting a cost benefit analysis is to find the best combination of controls that mitigate the greatest risks for the least cost. However, even with properly implemented controls and solid governance processes, risks may still remain. These are known as residual risks.

Risk Evaluation and Assessment

The risk evaluation and assessment component of the NIST risk guide focus on two components: good security practices and keys to successful risk management. The recommended good security practices include:

- Integrating risk mitigation into the software development life cycle
- Developing a schedule for assessing and mitigating risks
- Conducting risk mitigation studies when there are major changes in the IT infrastructure or when there are major changes to policies

The guide also identifies key success factors, many of which are common to other best practices and IT methodologies. These include:

- Commitment by executive and IT management
- Knowledgeable risk management team familiar with the particular IT environment as well as risk management methodologies
- Cooperation of users
- Ongoing evaluation and assessment practices

The Risk Management Guide for Information Technology Systems is a framework for addressing the problem of risk in IT systems. Unlike ITIL and COBIT, this framework is narrowly focused on one management process within IT. It does, however, demonstrate that specialized frameworks have much to offer IT management.

Leveraging SOM to Support Frameworks and Standards

The frameworks and best practices described in this chapter have distinct benefits and advantages. ITIL emphasizes the improvement of executing IT operations. COBIT tackles the problems of governance and control within IT. The ISO 17799 security standard and the NIST risk management guide focus on particular processes within IT. As diverse as these frameworks are, they have common characteristics and requirements.

These frameworks define repeatable processes that are broadly applicable to IT operations across industries. They define controls, goals, and metrics for implementing and measuring the effectiveness of those controls. They also leave implementation details to IT practitioners—and this is where SOM makes its contribution.

These frameworks are guides for running IT operations, but they depend on raw information about IT assets and processes. The ability to gather, analyze, and leverage that information is an outcome of SOM. SOM structures include a centralized change management database and a set of operationally oriented processes that parallel many of the tasks outlined in the frameworks described in this chapter.

Summary

There is no need to reinvent the wheel of IT management. Best practice frameworks, ranging from broad frameworks covering all major areas of IT management to more targeted guidelines, have been developed and are readily available for adoption by IT practitioners. These guidelines provide details about what should be done. The next chapter begins to analyze how to implement these practices using the tools of SOM.

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>.