Realtime
publishers
"Leading the Conversation"

The Definitive Guide™ To

Service-Oriented Systems Management

sponsored by

altiris®

Dan Sullivan

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 8: Leveraging Systems Management Processes for IT Governance

Throughout, this guide has examined systems management processes as they apply to controlling assets, processes, and procedures; providing service support; delivering services; and managing applications. This chapter turns your attention to a higher level of management and asks: How do you control and manage the implementation of these systems management processes?

What Is Governance?

Governance is the process of setting long-term objectives, establishing controls that measure the progress toward those objectives, and monitoring to ensure controls are followed and objectives are being met. In short, governance is about deciding what an organization should do, how to ensure it will get done, and then making sure it does get done. As Figure 8.1 shows, the governance process encompasses all aspects of service-oriented management (SOM).

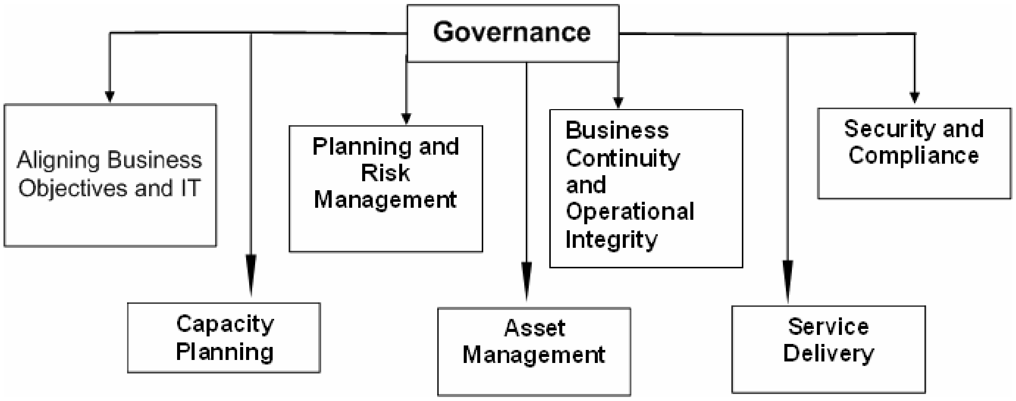
Governance
Aligning Business Objectives and IT
Planning and Risk Management
Business Continuity and Operational Integrity
Security and Compliance
Capacity Planning
Asset Management
Service Delivery

Figure 8.1: The governance process defines a framework in which SOM operations are controlled.

Let’s begin with an example that gives an overview of types of governance activities, including:

- Planning and organizing IT operations
- Acquiring and implementing IT solutions
- Ensuring proper delivery and support for IT solutions
- Monitoring services to ensure compliance with policies and procedures

When discussing each activity, let’s explore how to establish goals for each activity and how to measure progress toward those goals.

> The practices described here are industry standards that have evolved over the years. The best formalization of these types of best practices can be found in the Control Objectives for Information and related Technology (COBIT) framework established by the Information Systems Audit and Control Association (ISACA). More details about COBIT and ISACA can be found at http://www.isaca.org/.

Governance: An Example

Governance, as practiced according to COBIT, is a typical reductionist management practice. You first identify the parts of SOM, dividing them into logical groups, then continue dividing those groups into smaller and smaller constituent parts until the resulting units are easily described in terms of:

- What is to be accomplished?
- What factors influence the success of the objective?
- How can progress on the objective be measured?

For example, consider a company that has a strategic objective to reduce telecommunications costs by deploying voice over IP (VoIP). Doing so will require substantial investment of time and money, and the board of directors expects executive management to have a plan in place for overseeing the deployment of the VoIP system as well as ensuring that ongoing operations are meeting the organization’s needs within budget and on schedule. The process begins with planning how to acquire and implement the service. After the planning stage is complete, the process moves on to the acquisition and implementation processes. COBIT then provides a framework for delivery and support as well as monitoring and evaluation.

Planning a VoIP Implementation

For this example, assume that the IT organization responsible for implementing the VoIP solution is organized into several groups:

- Business analysis and project management
- Applications development
- Network services
- Server and client management
- Support services
- Training

Each will have a role in the VoIP project, so one of the first steps after defining the strategic plan that includes the project is to fit the project into the existing IT management structure. This includes:

- Determining how the project fits in the IT architecture
- Identifying the management processes that will control the execution of the project
- Incorporating the financial planning of the project into the broader IT investment portfolio
- Conducting a risk analysis of the project
- Planning the staffing and training requirements
- Executing established project management procedures

This process is controlled by involving business owners, project managers, and domain experts who will follow a formal planning process and document their findings, which are then reviewed and approved by executive management before proceeding to the next stage.

The business analysis and project management group as well as managers from network services and server and client management would have to be involved in the first step, determining how the project fits into the IT architecture. This same group would identify the management processes that will control the execution of the process. Now, ideally, that should be a relatively easy task. In a mature governance environment, those processes are well established.

> See the section "Governance and Maturity Models" later in this chapter for more information about the different levels of process maturity.

Incorporating the financial planning of the project and conducting the risk analysis are the responsibilities of the IT managers with assistance from business analysts, project managers, and domain experts. This group should also handle planning for staffing requirements and training. The final stage of planning is to formulate a project plan and engage management oversight of the project.

Each of the activities must be well documented. Common procedures, such as project planning and risk analysis, often have formal document deliverables that have a well-defined structure.

> Project management professionals have formalized their discipline and have developed a body of knowledge and a set of documents common to project management across domains, not just IT. For more information, see the Project Management Institute Web site at http://www.pmi.org/info/default.asp.

The deliverables from the planning stage should include project plans, risk analysis, and requirements documents. The governance process measures timeliness and quality to ensure that the planning process is working as expected. For example, key measures might include whether the documents were prepared on time, if the requirements document addresses the full scope of business and technical requirements, and whether the project plan met the standards outlined by the Project Management Institute.

Implementing a VoIP Solution

During the implementation phase, the emphasis shifts to selecting, acquiring, and installing the VoIP system. Selection is made based on a combination of functional requirements and feasibility analysis, which should include both technical and budget constraints.

Once VoIP hardware and software—as well as supplemental acquisitions such as additional network hardware and dedicated Internet bandwidth—are acquired, the implementation begins. This process begins with development and testing procedures and then rolls out to production.

The success of selection phases can be measured by the number of times business owners agree with feasibility studies and sign off on requirements as sufficiently comprehensive to proceed with the project. The measures of the deployment phase can include:

- Number and severity of bugs found in testing (reflects on the selection process)
- Number and severity of bugs found after deployment (reflects on the testing process)
- Number of days ahead or behind schedule for key implementation milestones
- Satisfaction of business owners and users with initial deployment
- Number of users trained on the system

After implementation of the service, the governance process will continue by controlling the maintenance and support for the service.

Maintaining and Servicing the VoIP Service

Once the VoIP system is operational, a new set of management objectives emerges:

- Managing service level agreements (SLAs)
- Managing third-party providers
- Providing service desk support
- Ensuring the availability of services
- Maintaining adequate security measures
- Training users
- Managing costs and charge backs

To ensure that these tasks are performed effectively, managers use a series of measures, such as:

- Number of times an SLA is violated
- Number of non-performance incidents with third-party providers
- Length of time the service was not available and number of users affected
- Number of security breaches that resulted in loss of availability, loss of confidential information, or corruption of data
- Number of users trained
- Total cost of OS, and per-user cost of system

The final part of the governance process is to monitor and evaluate IT processes.

Monitoring Operations

The final stage of the governance process is monitoring the delivery of VoIP services to determine whether objectives are being met. This could include analyzing summaries of the management reports generated as part of the operation maintenance. The objective isn't just to know how the service is performing but to know what is being done to correct any problems.

In practice, you do not perform governance over a single project or operation but over all IT projects and operations. This example illustrated the types of controls and measures that need to be in place to ensure that projects and services meet management expectations and, if they do not, that mechanisms are in place to make executive management aware of problems and provide them with enough information to address the problem. Let's move from the example to the formal structure of controls.

Governing IT Services

Governing IT services, according to COBIT practices, is divided into four parts:

- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring

Each of these areas is broken down into a set of control objectives, which in turn, have a definition, a method for achieving the objective, and suggested measures for determining whether the objective is being met.

Planning and Organization

The planning and organization phase of governance is subdivided into several areas:

- Defining IT strategic plan
- Defining IT architecture
- Defining IT processes and organization
- Managing IT investments
- Managing human resources
- Managing projects
- Managing IT risks

This section is not an attempt to cover all the topics addressed by COBIT. Some planning and organizational topics, such as controlling quality, are not covered. The purpose of this section is to describe governance and its relation to SOM. This chapter cannot, and does not attempt to, replace COBIT documentation.

Defining the IT Strategic Plan

The first step in planning for IT governance is to define an IT strategic plan. The plan is essentially a mechanism for aligning IT operations with business strategy. It should include:

- Descriptions of key business objectives and IT services required to realize those objectives
- Priorities assigned to each objective
- Plans for methods for keeping the IT strategic plan in alignment with changes in the business plan.

The plan should lay out what should be done by IT, not necessarily what is being done by IT. In addition, it must be understood that the plan is a dynamic tool for directing IT operations. IT management and executive management work closely to keep IT priorities in sync with changing business goals.

Defining IT Architecture

The planning and definition of an IT information architecture is one of the first points at which security emerges as a prominent aspect of planning. The information architecture of an enterprise includes:

- A organization-wide data model
- A data classification scheme
- Assignment of ownership of elements of the data model

Organization-Wide Data Model

The data model of the architecture should not be confused with the detailed and operation data models built during application and database development efforts. During the planning stages, the data model is more like an inventory of data elements than a structural description and is complete with dependencies and data integrity constraints. The data model should:

- Minimize redundancy of data
- Accommodate business functions needed to support strategic objectives
- Define common standards for data syntax to promote reuse
- Provide retention periods and destruction requirements

The data model becomes a reference point from which more detailed design and development projects can begin. By including data standards, the data model helps to promote interoperability between applications. The data model should also include a description of data retention policies. These policies may be based on government requirements (for example, in the case of tax information) or based on business practices (such as retaining non-regulated public information). The model should also include data classifications.

Data Classification Scheme

At the highest levels, business security classifications typically include:

- Public—The public classification is assigned to data that would not cause any adverse impact on the organization if it were released to the public. Obvious examples include information that has already been made publicly available, such as press releases, and data submitted to government regulators, such as annual and quarterly security reports, including 10-Ks and 10-Qs in the United States.
- Sensitive—Sensitive information should not be released publicly to protect the interests of the organization; however, if it were released, the damage would be minimal. Financial information, vendor negotiations, project plans, and other information that is often widely dispersed within an organization fall into this classification. There are, of course, matters of degree that must be taken into account. Financial information about a pending merger that has not been disclosed could adversely affect share prices or prompt strategic reaction from competitors.
- Private—Private information is information about persons involved with the organizations, such as employees, customers, patients, and clients. Private information is the subject of many regulations, from the European Union's Privacy Directives to the United States' Health Insurance Portability and Accountability Act (HIPAA) regulation on healthcare information to state level regulations such as California's SB 1386.
- Confidential—Confidential information requires the greatest protection because its disclosure could have significant adverse impacts on the organization. Examples include:
    - Trade secrets
    - Proprietary process plans
    - Strategic negotiations
    - Strategic plans

  Significant controls should be in place to protect both the confidentiality and integrity of confidential information.

Security measures should be sufficient to protect information appropriate for its classification level.

Data Ownership

A role of data owner should be defined for each element of the data model. The business owner is the person responsible and accountable for the management of that data. The business owner role is typically filled by an executive or management role; it is not the systems administrator or database administrator who may be responsible for the day-to-day maintenance of the data and the infrastructure that supports it. Data owners are responsible for:

- Formulating policies and procedures controlling the use of the data
- Meeting regulatory requirements concerning the data
- Defining security, availability, and business continuity requirements regarding the data

The information architecture is one of the areas of COBIT that has direct impact on systems management operations; another is defining IT processes and organization.

Defining IT Processes and Organization

The most effective systems management operations are based on well-structured processes and organizations. The planning of IT operations begins with defining areas of responsibility, creating roles, and formulating policies and procedures for conducting the organization's IT operations.

COBIT identifies several specific functions that should be addressed in a process and organization plan:

- Control of operations
- Quality assurance
- Risk management
- Security
- Data ownership
- Segregation of duties

Another aspect of the plan is the structure of IT operations. To effectively control IT operations, the structure should be based on business needs and technical requirements. For example, from a business user perspective, a mission-critical application needs to be available 99.999 percent of the time. From a technical perspective, this requirement maps to several technical requirements, ranging from storage capacity and network bandwidth to application design and access controls. It is highly unlikely that one would organize IT operations around an application. The types of services utilized by the applications, such as storage, networking, and servers, are more likely to align with staff skills and a manageable division of labor.

Most of the elements of the process and organization plan are addressed elsewhere in this guide, but segregation of duties has not and deserves attention. This is one of the most important aspects of security management but is a far less popular topic than other more technically interesting issues.

The principle of separation of duties is that more than one person is required to complete a critical task. For example, a developer may program a change for an application that is then tested by another person who then passes on the tested code to a third person for release. Developers would not have access to the test environment, and only release managers can move code into production. In this way, at least two roles would have to collude in order for a piece of malicious code to work its way into the production environment. The other areas of planning and organization center on the management of the IT organization rather than on the services it provides.

Managing IT Investments

Managing IT investments can be boiled down to one word: budgeting. Given a set of strategic directives, IT executives are expected to deliver the services needed with the financial resources allocated. This process is more than just balancing funding and expenditures, it includes:

- Allocating funds to specific operations and projects
- Creating financial forecasts and optional scenarios
- Establishing criteria for measuring the value of proposed projects
- Monitoring the value of ongoing projects

Managing investments is highly dependent on proper management of human resources and projects.

Managing Human Resources and Projects

Managing human resources includes the typical operations one would expect, such as:

- Hiring and terminating employees
- Training
- Conducting personnel reviews and assisting with career planning
- Defining job roles and responsibilities
- Supporting the use of contractors and consultant to augment permanent staff

Having the right combination of skills within an organization is critical to maintaining ongoing operations and properly staffing projects.

Project management includes elements of human resource management as well:

- Defining project management frameworks that explain stages of project management and documentation required for each stage
- Creating project management guidelines
- Providing oversight of projects

Oversight is essential to detecting problems with project deliverables. Identifying and correcting problems in projects early can limit the costs and risks to the project. Risk management, though, extends well beyond tracking the timeliness of project schedules.

Managing IT Risks

Risk management, like project management, should be done within a formal framework. IT, by nature, has risks not present in other business areas. The potential for system incompatibilities, security threats, and the disruption of operations can occur on a substantial scale with relatively little input. For example, a single attacker could breach a database application and steal tens of thousands of customer records, or a single failure in a critical network device can disrupt multiple operations.

Managing IT risks includes:

- Defining a risk management framework for determining risks and identifying the organization's level of risk tolerance
- Conducting risk assessments
- Formulating risk mitigation plans

By creating a formal management structure that includes all the essential elements outlined, an IT organization will have a strong foundation for moving to the other areas of IT operations, such a the acquisition and implementation of IT services.

Acquisition and Implementation

Acquiring and implementing IT solutions is an ongoing process. From a SOM perspective, these activities constitute a major part of the systems management process. The major tasks in this stage include:

- Evaluating and selecting solutions
- Acquiring and maintaining both hardware and software
- Enabling operation and use
- Managing change

These tasks constitute the major parts of a system life cycle and so, not surprisingly, the controls governing these tasks are essentially the same as those found in development methodologies.

Evaluating and Selecting Solutions

When a perceived business need for an IT solution is recognized, a formal evaluation and selection process should begin. The process should include:

- Soliciting functional business requirements
- Defining technical requirements, such as capacity, security, and other non-functional requirements
- Conducting risk analysis and feasibility studies for the project
- Receiving executive approval for the proposed solution and prioritizing the implementation along with other IT initiatives

The evaluation and selection tasks entail what is often called the “build vs. buy” decision. This is something of a misnomer because complex systems are can rarely be reduced to such a simple dichotomy. In practice, the decision is more akin to selecting a point on a continuum ranging from buying a turnkey solution to building a custom solution for every aspect of a system.

For example, in the case of the VoIP example from earlier in the chapter, the systems designers and project sponsors may conclude that no commercially available system meets all needs. The same group is likely to conclude that “building” a VoIP solution is not feasible. The solution in such cases involves starting with a commercial application as a base and customizing applications as needed and integrating with existing infrastructure to get the functionality required. This is done during the acquisition and maintenance phases.

Acquiring and Maintaining Systems

The acquisition phase of IT systems management is a relatively high-risk area. It is at this point that solutions are implemented, software is developed, hardware acquired, and the impact of poor planning and incomplete requirements starts to come to light. Thorough management is required to keep projects on track, plan for contingencies, and be able to respond to roadblocks that can derail a project.

The term “death march” has come into software development parlance to describe a project that will inevitably fail. The failure is often due to a combination of poor planning, poor project management, insufficient resources, changing requirements, and unrealistic schedules. All these factors can be avoided, or at least mitigated, by proper governance procedures.

Managing this phase of IT operations entails:

- Mapping functional and non-functional requirements into sufficiently detailed designs so that implementations can be carried out without the risk of unanticipated conflicts, missed dependencies, or other factors that can compromise the progress of the project.
- Following software development practices suitable for the type of project underway. Some methodologies, such as extreme programming, may be appropriate for small projects or parts of projects, while a spiral methodology may be required for larger multi-faceted projects.
- Using appropriate division of development, testing, and production environments.
- Ensuring change management and release management practices are followed.
- Planning for capacity and availability requirements so that suitable resources are in place when applications are deployed.

As with other stages, the acquisition and implementation phases have overlapping characteristics with the next phases—enabling operation and use.

Enabling Operation and Use

The process of enabling operation and use focuses on the release management process that moves a system from development and testing into production. The steps of this process include:

- Developing administration and end-user documentation for the system
- Developing training material for administrators and end users
- Planning the roll out of client applications
- Planning the roll out of server-side applications
- Coordinating any operational transitions for existing processes and systems to the new application and related processes

This is also a relatively high-risk part of IT management processes, but the level of risk is directly proportional to the amount of planning and the quality of development efforts that precede it. When developers follow established software engineering practices, comprehensive testing and defect management is in place, and the rollout of applications is coordinated with business partners, then the risks in the transition to production are reduced. Poor programming, inadequate testing, lax management of the systems life cycle, and ad hoc procedures for releasing an application is a recipe for disaster. Once systems are in place, the management focus turns to maintenance operations; one that requires formalized procedures is change management.

Managing Change

Changes made on an ad hoc basis are more likely to succumb to a common scenario. It begins with an urgent requirement coming to light or the discovery of a flaw in a program. Due to a sense of urgency, rather than follow formal analysis, design, development, and testing, it is decided that a developer can start with a minimal summary of requirements (which are rarely documented). The developer makes a change that addresses the immediate problem, or at least corrects the symptom of the problem, with the good intention of going back into the code and fixing it the right way when he or she has more time. Formal testing procedures are bypassed and after a few unit tests followed by a minimal integration test, the code is moved to production.

What follows from that point can vary, but some of the outcomes are:

- The patch itself has a bug that was not detected during the minimal testing that was done
- A new bug indicates an unanticipated dependency in another part of the code, which was thought to be unrelated to the section that was patched
- The patch, while programmed according to the system documentation, fails to work correctly because of a previous ad hoc patch that changed a function but was unknown because the follow-on step of updating the documentation wasn't performed

This type of disruption to operational systems can be avoided by:

- Using established testing methodologies
- Reviewing changes with a broad set of developers, administrators, and key users before implementing the change
- Documenting the change process
- Conducting post-implementation reviews to determine ways to improve the process

A well-established change management procedure is essential for managing the next stage: delivery and support.

Delivery and Support

Delivery and support is, in many ways, the heart of systems management. Much of the effort of systems managers is directed to several key processes:

- Managing service levels
- Maintaining performance and capacity levels
- Ensuring security of systems
- Managing budgets and resources
- Providing training
- Providing service support
- Managing data
- Managing the physical infrastructure

Together these activities provide the systems management foundations for the day-to-day operations of business systems.

Managing Service Levels

Business owners of a system and systems administrators should have a common understanding of the expectations for the service levels of the system. Ideally, this is worked out during the requirements and design stages, but realistically, it typically needs adjustment as an organization gains experience with a system and adapts to changing trends in system demands. These agreements are formalized in SLAs and operational level agreements (OLAs). Some of the factors included in SLAs are:

- Service availability
- Capacity of services
- Performance levels
- Service support response times
- Continuity plans
- Security requirements

The SLAs address what is to be provided, and the OLAs focus on how service levels will be met with particular hardware, software, network, and staffing resources.

Maintaining Performance and Capacity Levels

SLAs provide the metrics that systems administrators use to allocate resources. To maintain performance levels, systems administrators must:

- Monitor response times
- Collect related performance statistics (for example, CPU usage, bandwidth usage, and so on) when performance levels are not reached
- Report on performance levels so that management can adjust resources as needed
- Develop forecasts of future demands on the application

Closely related to performance management is capacity management. The difference is that instead of focusing on the response times, capacity management focuses on underlying resources required to maintain service levels. The tasks in this area include:

- Monitoring CPU, disk, and network use
- Assessing the impact of a change in requirements; for example, the time and space required to perform additional backups
- Forecasting trends in resource use

Another task essential to the viability of service levels is ensuring the integrity of applications and data.

Ensuring Security of Systems

Security is a multifaceted challenge, and governing the security management process is equally as complex. The fundamental goals of information security are to maintain the confidentiality, integrity, and availability of systems and data. To meet this objective, well-managed IT organizations will:

- Document security requirements relative to business requirements
- Establish identity management and access controls
- Review government regulations and establish procedures to ensure compliance
- Establish monitoring and auditing procedures
- Establish incident response policies and procedures
- Change control procedures
- Establish security configuration standards

Security entails a balance between the need to protect information and assets and the need to keep resources accessible to users without unnecessary burden. To strike a proper balance, the business requirements, relative to security requirements, should be well documented. This begins with data classification. Identity management and access controls will build upon the information classification scheme described earlier. By first portioning information into different categories, it is easier for security managers and systems administrators to properly apply access controls. Other requirements, such as the need to share information with business partners, can extend beyond the boundaries of the organization.

Government regulations drive a wide array of security requirements and have helped to promote the practice of IT governance. At the very least, organizations should understand which regulations apply to the operations and then review policies and procedures in light of those regulations. In some cases, such as the Sarbanes-Oxley Act, auditors can help formulate appropriate controls to meet regulatory requirements.

Monitoring and auditing policies are required as well. Governance depends on measures to assess the effectiveness of controls, so one would expect security management to require monitoring for that reason alone. More importantly, monitoring is an active part information security practice; it serves multiple purposes, ranging from helping detect anomalous events to providing traces of events that occur during a security breach.

Finally, the governance of security operations should include the establishment of incident response policies and procedures. Executives, managers, systems administrators, network managers, and others should all know their roles and responsibilities in the case of a security breach. Well-defined reporting procedures should be established. Key measures of system security management include the number and severity of security breaches and the number of times security requirements are not met.

Managing Budgets and Resources

During the planning process, budgets are established and priorities set. During the delivery phases, the focus shifts from the high-level allocation of resources to tracking expenditures and charge backs. The goal is to ensure that charges are properly allocated and costs recovered and that projects and services stay within budget.

The Problem with Charge Backs

One of the trickiest areas of financial IT management is allocating costs. Ideally, the business units that use services pay IT costs; and they pay according to the levels of services they receive. In practice, distortions in cost can occur.

Consider the example of a storage area network (SAN) used by several departments. The IT department purchases or leases the disk array for a period of 3 years and charges each department according to the amount of storage used. The costs of the hardware, software, service, and support staff are known for the 3-year period, so the IT department calculates the lifetime cost of the service. Each department is charged for the percentage of the storage they use on a per-gigabyte-of-storage-per-month basis.

Thus, if five departments use equal amounts of storage, they each pay the same amount. Suppose that one of the departments decides to use another storage service or no longer needs as much storage. The IT department is charging less because less storage is used, and so they are no longer recovering their costs. Does the IT department increase charges to compensate for the lost charge backs? If it does, the other departments will bear the increased costs leading them to either reduce their storage use or look elsewhere for storage services. If the remaining departments reduce their storage use, the cycle continues, and the IT department would have to increase per-unit charges again to recover costs.

Internal charge-back models must be carefully formulated to avoid distorting reasonable economic incentives. Some balance must be found to meet the objectives of individual departments while realizing the benefits of economies of scale. Key measures of the success of a charge-back system is the number of times charge-back costs are disputed and the number of times service agreements are either terminated or not renewed because of cost disputes.

Measuring Variance

Budgets will vary from actual expenditures; how often this happens and to what degree is another measure of the budgeting and allocation management process. When measuring variance, management should determine an appropriate aggregate level.

For example, within a department, a line item for one activity, such as payroll and benefits, may be over budget but another comparable line item, such as consulting fees, may be sufficiently under budget to compensate for the difference. This may or may not be a cause for concern. Consulting fees within the budget may be highly variable, while payroll costs tend to be less so. If consulting fees are reduced in the next budget cycle, what will offset the ongoing increased payroll charges?

Another type of variance that should be monitored by the governance process is the reallocation of funds to different types of expenditures. For example, a decrease in spending on service contracts to compensate for overruns in other line items could leave some services vulnerable to disruption or subject to lower performance levels than defined in SLAs.

Providing Training

Training is a fundamental IT service. For overall governance of training, the following are key measures:

- Number of users trained
- Rate of service desk calls related to functions addressed in training
- Subjective quality ratings provided by trainees

Effective training is correlated with the demands for service support.

Providing Service Support

Service support provides users with someone to turn to when problems or questions arise with IT applications. Successful service support requires

- Adequate capacity of first-line support personnel to field calls
- Appropriately trained support personnel who can handle the majority of calls within the first and second levels of support
- Escalation procedures for determining when to seek more specialized assistance with a particular problem
- Management procedures for collecting data about service calls to identify trends and spot potential weaknesses both in applications and support services

The quality of service support can be measured with quantitative measures, such as the number of calls per service desk employee, the average time to resolve an incident, and the number of incidents escalated to higher levels. Qualitative measures, such as users' satisfaction, can also be used.

Managing Data

Backup and recovery operations are required to preserve the availability and integrity of data. Although the topic sounds mundane and rather simple at first, the complexities of backup become clear quickly. Some of the topics that must be addressed in backup policies include:

- Determining what to back up—Data is frequently duplicated for performance purposes or for ease of integration. What data source is considered the system of record (that is, the definitive record)?
- Adequately protecting backup data—For example, what data classifications should be encrypted when backed up?
- How long should data be retained?—When data is removed from operational systems according to records retention policies, how will copies of the data be deleted?
- Backup media is subject to failure like any other device—How much testing of backup and archive material is required?

This service may be measured by the number of times backups are successfully performed and the percent of time backups are performed in the time allotted to the backup process.

Managing the Physical Infrastructure

Many of the governance topics focus on managing the technical aspects of IT services and controlling organizational factors, such as budgets and staff. Another important topic is managing the physical infrastructure of an IT operation. This includes

- Providing adequate facilities—including space, power, and environmental controls—to accommodate staff and hardware
- Supporting contingency planning by having offsite or backup facilities in the case of service disruption at a primary location
- Deploying physical security controls at facilities

Measures for this area include tracking the number of security breaches at a facility and the number of lost hours due to power failure or loss of other required utility.

Delivering and supporting IT operations is a multi-faceted challenge. By dividing the tasks in the logical divisions outlined and tracking progress with some of the measures provided, an IT organization can build on past experiences to improve on service delivery.

Monitoring and Evaluating IT Management

Monitoring and evaluation processes are not limited to the technical or human resource aspects of IT. The IT management process itself should be monitored and measured. This process includes steps such as

- Analyzing performance reports to understand the overall state of IT operation
- Assessing how well SLAs are being met overall
- Reviewing exceptions to management frameworks
- Monitoring the state of regulatory compliance
- Conducting self evaluations, including quality surveys of customers

Again, the objective is to establish a set of policies and procedures and then measure the level of adherence to those policies and procedures. The monitoring process for IT can provide indications of management processes that need correction.

Governance and Maturity Models

This discussion of governance has outlined the major areas of IT management and divided those into logical manageable units with key measures for determining how well each is managed. The measures also provide indications of trends, weak areas, and other factors requiring management attention. It must be recognized, though, that not all organizations are at the same level of capability to monitor their management processes.

Examples of Varying Levels of Capability Maturity

Consider some scenarios that impact the ability of an organization to provide effective governance of IT operations:

- An organization without a well-defined strategic plan cannot align IT objectives to business objectives.
- Without standardized procedures for managing projects, it is impossible to compare the performance of multiple projects to determine which factors promote and which hinder project deliverables.
- A development team does not have a distinct test environment or team of quality control testers, so they perform their own testing in a development environment before deploying code.
- Training of systems administrators on new applications is not a formalized process; developers typically spend a brief amount of time with systems administrators just prior to deployment to explain how the system works and what is required to manage it. Formal documentation is not produced.

These examples all depict organizations at different capabilities for governing IT operations. In the first scenario, the organization is incapable of governance because there is no foundation upon which to build an IT strategy. IT managers are left to respond to ad hoc requests for services and are likely juggling multiple projects with no priorities to order those initiatives. The result of this type of management scenario is a group of frustrated users and business managers and an IT staff in “fire drill” mode.

In the second scenario, the organization recognizes the need for management frameworks but does not have a consistently applied methodology for project management. Although some project management is better than none, every project may be managed differently, varying according to the management style of the person in charge.

Inadequate resources hamper the development team in the third example. The team is forced to conduct two distinct activities, testing and development, in the same environment. This can lead to conflicts in the use of resources, introduce dependencies that would not exist if separate environments were used, and can delay deliverables as tasks are scheduled around the limited resources of the development environment. In addition, testing sizable software development efforts require a formal methodology; many developers are not trained in those methodologies. The result is, good intentions aside, inadequate testing that leads to higher risk of failure during deployment.

The final scenario depicts a lack of emphasis on operational support. Without proper training and support, systems administrators will not be able to effectively manage and tune an application. Users may not receive or may be delayed in receiving the services they need. These kinds of scenarios show that adopting sound management frameworks and development methodologies is not black and white (as in, either you do it all or you do not do it at all); rather, there is a continuum with many processes within many organizations somewhere between the best and worst extremes.

Capability Maturity Models

The Carnegie Mellon Software Engineering Institute (SEI—http://www.sei.cmu.edu) has developed a formal model for measuring the level of maturity of an organization with respect to processes such as software development. These are known as capability maturity models and define levels of control and optimization that an organization is capable of exercising. The maturity models are divided into six stages of development:

- Level 0 (Non-existent)—At this level, there are no discernable processes of systematic management.
- Level 1 (Initial)—At this level, projects, issues, software development, or other key processes are managed on an ad hoc basis. There is little or no connection between how a process is carried out in one instance and another. There is no coherent management process.
- Level 2 (Repeatable)—At this level, there is some common understanding of how to perform tasks, but there is no formal documentation or training on the processes. At this stage, success or failure is highly dependent on the capabilities of the people immediately involved in the process.
- Level 3 (Defined)—At this stage, procedures have been formalized and documented. Participants receive training in the process. There is little oversight, though, to ensure that the process model is followed.
- Level 4 (Managed)—This stage builds on level 3 by adding more management oversight.
- Level 5 (Optimized)—Processes are well managed, compliance with standards is measured, and results are measured and used to tune processes.

This framework uses a set of key performance goals and key performance indicators to guide the implementation of the COBIT objectives. Key goal indicators measure how effectively an organization achieves its goals. Key performance indicators measure specific operations and processes and are leading indicators of the organization's trend toward reaching its goals. Key goal indicators measure overall performance with respect to a goal after the fact. In addition, key performance indicators are measures gathered during the observation period and thus allow time for management to adjust practices and make corrections as needed.

> 🕮 For more information about maturity models and management, see the SEI documentation at http://www.sei.cmu.edu/managing/managing.html.

Organizations that start to implement formal governance procedures will do so at some point in the maturity model. If, for example, executive management has decided to improve the software development process, which is currently at some point between Level 1 and Level 2, then one of the first objectives will be to formalize documentation and training. Governance measures should also focus on allowing management measures to progress toward those goals. Implementing governance procedures must be done with recognition for the relative capability maturity of the IT organization.

Summary

Governance is the process of directing and controlling operations to ensure that long-term objectives are met. COBIT is a deep and broad framework for implementing governance best practices. The IT field is mature enough that management and governance practices need not be an exercise in reinventing the wheel; rather, the goal of executives and IT management should be to find frameworks that serve the needs of the organization and work well together. SOM, for example, is highly amenable to governance because of the logical organization of operations and resources and the focus on measuring performance. It should be understood that governance is an ongoing process that will change as the maturity level of the IT organization changes. As systems management, software development, and training procedures improve, it is likely that the ability to keep those aligned with strategic objectives will improve as well.

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.