Operations Management Capabilities Model

Edward Wustenhoff, Sun Global Datacenter Practice, Client Solutions

Michael J. Moore, Sun Global Datacenter Practice, Client Solutions

Dale H. Avery, Sun Educational Services

Sun BluePrints™ OnLine—February 2005

http://www.sun.com/blueprints

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95045 U.S.A.
650 960-1300

Part No. 819-1693-10
Revision 1.0, 1/14/05
Edition: February 2005

Please
Recycle

Contents

1

Part 1—Introduction

Part 1 of this document provides an executive summary and introduces the concept of operational capability, the capabilities model described in this document, and compares it with other industry standards and models. Part 1 contains the following chapters:

- Chapter 1, “Executive Summary”
- Chapter 2, “Introduction”

1

Executive Summary

Today's IT organizations are under pressure to meet or improve IT service levels for critical business functions despite shrinking budgets and amidst organizational, process efficiency, and automation challenges. In an effort to provide consistent and predictable levels of service to their respective organizations, IT departments have invested heavily in technology resources (people, processes, and tools) to manage the extended data center. Despite this investment, many firms are still not able to effectively manage the IT environment and meet the service level requirements for users of the organization's IT products and services.

Successful IT management cannot be purchased out-of-the-box. Implementation of a robust IT management infrastructure is as much an exercise in organizational change as it is a technology implementation. Operational capability is therefore acquired in an evolutionary manner, over time, through the application of a continuous improvement methodology that addresses the combination of people, process, and tools components.

Various industry standards, such as the IT Infrastructure Library (ITIL) and the Controls Objective for Information and Related Technology (COBIT) standard, have gained wide acceptance as comprehensive methodologies for improving the effectiveness of IT management. What these methodologies lack, however, are specific metrics that can be used to measure and assess—in an objective and consistent manner—the effectiveness of IT management in an organization.

This document introduces the Sun Microsystem's *Operations Management Capabilities Model* (*OMCM*), a comprehensive, continuous improvement methodology for IT management that:

- provides a practical framework and measurable roadmap for enhancing IT management
- encompasses IT management best practices at all levels of the IT environment
- helps define, measure, and thoroughly assess, an organization's current IT capability as well desired future capability
- maps IT management disciplines to the architecture used to implement it

- provides the basis of assessment for the purpose of determining where best to invest in IT resources in support of key business needs

The OMCM is based on the *Sun IT Management Framework* (*Sun ITMF*), which defines the three different aspects—people, processes, and tools—of an organization's IT management infrastructure. The people aspect represents the skills, training, management, and discipline required to effectively and efficiently execute the processes and run the tools to support the IT lifecycle and automate the IT management processes. The process aspect represents the actual IT management processes used to support the IT service life cycle. The tools aspect represents the actual technology used to facilitate and automate the execution of the various IT management processes.

This document consists of the following parts:

- Part 1, "Introduction," defines the concept of operational capability, introduces the operations management capabilities model, and surveys related industry standards and models.
- Part 2, "Sun IT Management Framework" (Sun ITMF) introduces the Sun ITMF and describes, at a high level, its core aspects—people, processes, and tools.
- Part 3, "Operations Management Capabilities Model (OMCM)," is the OMCM specification that introduces the OMCM, delineates the various levels of IT operational maturity and describes the people, process, and tools aspects of the OMCM. It provides various ways to measure IT capability—degrees of implementation (ad hoc, emerging, functional, effective, and optimized), critical factors to measure, assessment criteria, and metrics that provide predictive or descriptive measures.
- Part 4, "Conclusion," describes how the OMCM can applied within an organization.

2

Introduction

This chapter introduces the Operations Management Capabilities Model (OMCM). It includes the following sections:

- About This Document
- Concept of Operational Capability
- Operations Management Capabilities Model
- Other Industry Standards and Models
- What This Document Contains

About This Document

This document provides a comprehensive overview of an Operations Management Capabilities Model (OMCM) developed by Sun. It provides the following information:

- background information on the development of the model
- the motivations for building the model
- taxonomy of the various levels of the OMCM
- description of the IT management framework that is used as the basis of the capabilities model

Note – Throughout this document, terms are defined within the context of the OMCM and the Sun IT Management Framework (Sun ITFM). Such definitions represent Sun's *interpretations* of industry standard terminology. We provide definitions to ensure that terms are used consistently and to set the proper expectations for what is—and what is not—specified in this document.

Concept of Operational Capability

In an effort to provide consistent and predictable levels of service to the organization, IT departments have invested heavily in technology to manage the extended data center. According to IDC[1], worldwide spending on systems and storage management software was approximately $13.3 billion in 2001.

Despite this heavy investment, many firms are not able to effectively manage the IT environment. Surveys and estimates from a variety of sources indicate that few organizations actually *deliver* (defined as *putting a solution into production*) an enterprise management project. Even fewer *succeed* (defined as *having the solution meet or exceed expectations*) with the effort. Past surveys from Gartner[2] reveal that enterprise event console implementations have a completion rate of 40% and a success rate of 20%. Although the Gartner research is dated, there is little to indicate that this has changed significantly in the past five years.

The growing realization that management cannot be purchased out-of-the-box has led to increasing interest in IT operational processes. Various standards, such as the IT Infrastructure Library (ITIL) and the Controls Objective for Information and Related Technology (COBIT) standard, are used extensively in Europe to improve effective IT management and are rapidly gaining acceptance within the United States.

Finally, there are always ongoing efforts to address the people who manage the IT environment, with one of the latest trends being the shifting of IT development and support activities to lower cost locations overseas. When this is done, there should be a standard against which the overseas IT delivery / IT delivery team can be measured.

All of these efforts on the part of IT organizations are focused on providing value to the organization. However, the desired result is not necessarily an operational monitoring environment or a robust change management process. As the old adage says, a person who buys a shovel does not really want a shovel—they want a hole in the ground. The same holds true for organizations that make investments in enterprise management technology, process implementation, or staffing. What is actually being purchased is the ability to *meet the service level requirements* for both internal and external users of the organization's IT products and services. The people, process, and tools are simply a means to acquire this capability.

1. *Worldwide Enterprise System Management Software Forecast and Analyst Summary 2002 2006*, IDC Bulletin 27402, 2002.

2. *Effectively Managing Event Console Implementations*, Gartner Group Document COM-03-6600, May 1998.

In this document, we define *operational capability* as:

> The combination of people, process, and tools that provides an organization with the ability to deliver IT services to an agreed upon service level in a predictable fashion with acceptable risk and cost.

The following figure provides a visual representation of the interaction among the process, people, and tools components that results in an organization's operational capability.

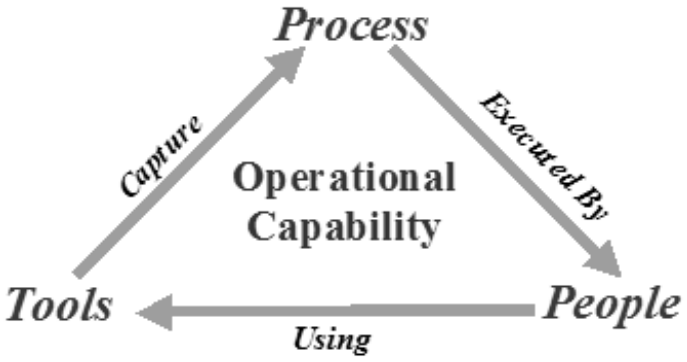

FIGURE 2-1 Components of Operational Capability

Our working definition of operational capability helps us identify what it is we want. Now, how do we acquire it? As experience has shown, an organization cannot simply buy operational capability through investments in technology. For example, the enterprise management framework, which used comprehensive enterprise systems management applications to measure IT's capabilities, resulted in many failed experiences for organizations during the late 1990s.

Because the components of operational capability include not only tools but also people and process, it is very difficult to acquire operational capability through a revolutionary or big bang approach. Implementation of a robust IT management infrastructure is as much an exercise in organizational change as it is a technology implementation.

Therefore, operational capability is something that is acquired in an *evolutionary* fashion over time. Operational capability cannot be obtained through the completion of a single project or technology investment. It is developed in an evolutionary manner through the application of a continuous improvement methodology that addresses the combination of people, process, and tools components.

Operations Management Capabilities Model

Experience has shown that IT organizations pass through a series of stages or levels as they improve their operational capability. Because—at a high level—different organizations are working on the same problem (operational capability), this evolutionary process is somewhat consistent. A large part of this consistency is driven by the dependencies that exist among the various parts that make up the process, people, or tools components.

For example, most organizations will not be driven to implement an event management solution—the "single pane of glass" or "manager of managers" solution in which a single console is used to aggregate information from multiple lower level management systems—until the underlying components of the solution have been deployed. The service level management process is difficult to implement successfully unless there exists a set of associated change, asset, and incident management processes. There are also dependencies across the components of operational capability. Successful deployment of a service level management tool requires that a corresponding set of Service Level Agreements (SLAs) be managed to. Such SLAs will probably not exist unless a service level management process is in place.

We believe that operational capability develops in a consistent fashion over time, and we feel that it is possible to produce a model of operational capability. In this document, a *model* is defined as *a schematic description of a system or theory that accounts for its known properties*[3].

Such a model has a number of potential uses. At a minimum, a capabilities model can help define the problem of managing the IT environment by capturing the entire problem space and providing a common framework for its analysis and discussion. Therefore, the model serves as a communications vehicle that allows different parts of the organization to describe both the current state of IT capability and a desired state.

A capabilities model also serves as the basis of a continuous improvement methodology. By describing a series of steps in the evolution of operational capability, the model supports the development of an architecture and the roadmap to realize it. This model is an attempt to capture the experiences of the industry in the development and deployment of IT management infrastructure. By specifying a logical sequence of activities, the model helps organizations to focus investment.

3. *The American Heritage Dictionary* (Third Addition), Dell Publishing, New York, NY 1994.

For organizations like Sun, the capabilities model provides the basis of assessment and remediation services that may be offered to customers as they attempt to improve the availability of key systems, applications, and services. Availability cannot just be purchased. It must be planned for and managed. The availability of critical systems is a function of the soundness of the deployment architecture, the reliability of the building blocks (hardware, software, network), and the capability of the organization to deploy, manage and protect them. Vendors do their customers a disservice when they attempt to solve availability issues by focusing on one of the aspects to the exclusion of the others.

In order to be useful, this model needs to define, at some level, the components of operational capability, their relationships, and the evolutionary path that is followed to acquire and integrate them into the organization. The model needs to be improvement focused with clearly defined requirements for each step. The model should also be specified with sufficient detail to support practical application by IT professionals. However, too much detail can make the model inflexible and communicate a level of accuracy that might not exist. Therefore, a certain level of ambiguity is present by design to allow the model to be applied in a wide variety of roles and situations.

We name this model the *Operations Management Capabilities Model* (or *OMCM*) to reinforce two ideas:

- This model predominately deals with the *operational infrastructure*. We reference the business and application delivery environments as necessary to set context or identify requirements, and process interfaces. As will be described in the chapters on the management framework, we draw a clear line between the three areas.
- This model makes the distinction between *capability* and *maturity*. In some cases, both terms are used interchangeably when discussing the evolution of IT operations. However, we believe there is no particular advantage in having a mature environment. Over the years, many mature organizational processes have been found to be inefficient or downright dysfunctional. We believe that the term *capability* better defines the reason for investment.

Other Industry Standards and Models

The idea of operational capability or maturity is not a new one. A number of industry initiatives and standards introduce and use the idea that capability is developed in a defined pattern over time. In fact, we have leveraged concepts and details from some of these models in the development of the OMCM.

This section briefly describes two different maturity models:

- Gartner IT Process Maturity Model
- Vrije Universiteit IT Service Capability Maturity Model

Other maturity models were also reviewed, including the Model specified in the COBIT Management Guidelines[4] and other work by the Software Engineering Institute, such as the Software Capability Maturity Model (CMM).

Gartner IT Process Maturity Model

Gartner[5] has developed a IT Process Maturity Model that identifies five levels of IT maturity, as summarized in the following table.

TABLE 2-1 Gartner IT Process Maturity Model (Gartner Group 1999)

Level	IT Process Maturity	Description	Estimated Distribution of Organizations
4	Value	IT organization and metric linkage; use of management and applications to improve the business process; enhanced cost recovery.	<1%
3	Service	Capacity planning and service level management.	<5%
2	Proactive	Performance, change, problem, and configuration management; automation, job scheduling, and availability management.	10%
1	Reactive	Basic event up-down, console management, trouble ticketing, basic backup and recovery, and basic topology.	60%
0	Chaotic	Multiple unconsolidated help desks; users identify problems; minimal IT operations.	24%

4. *COBIT Management Guidelines* (Third Edition), IT Governance Institute, July 2000.

5. *IT Process Maturity*, Research Note DF-08-6312, July 22, 1999.

The basis of the Gartner model is that organizations evolve through the various process maturity levels. Gartner estimates that mainframe shops took 10 to 20 years to reach the Level 3 (“Service” level) of the model described in the previous table. Information Services shops supporting distributed systems have not had as long to mature. Because the numbers are from 1999, it is safe to assume that the distribution of organizations has drifted more towards Level 2, driven by the need to operate mission critical distributed applications for eBusiness and other functions. However, it is our contention that a majority of the distributed IS organizations are still below Level 3.

Vrije Universiteit IT Service Capability Maturity Model

In December 1999, F. Niessink and H. van Vliet of Vrije Universiteit[6] published a paper describing a maturity model for IT service capabilities based on the Software Engineering Institute's Software Capability Maturity Model. Like Gartner, Niessink and van Vliet defined a model with five discrete levels, as described in the following table.

TABLE 2-2 IT Service Capability Maturity Model (F. Niessink and H. van Vliet 1999)

Level	IT Process Maturity	Description
5	Optimizing	Continuous process improvement is enabled by using captured metrics and from innovation.
4	Managed	Metrics on the service process are captured. Service delivery processes and services are quantitatively understood and controlled.
3	Defined	IT processes are documented, standardized, and integrated into a standard service process. All services are delivered using variations of the approved, standard service processes.
2	Repeatable	Basic service management process is in place. It is possible to repeat success on similar services with similar service levels.
1	Initial	The service delivery process is characterized as ad hoc or chaotic. Few processes are defined and success depends on individual efforts and heroics.

6. *The Vrije Universiteit IT Service Capability Maturity Model*, Technical Report IR 463 Release I.2-1.0, Frank Niessink and Hans van Vliet, December 1999.

The model uses the same basic structure as the Software CMM. A maturity level contains key process areas, which are organized by common features that are defined by key practices. At the time of this document's publication, the process maturity levels had been defined only up to Level 3 (Defined Maturity Level).

The IT Service Capability Maturity Model defines two key characteristics that we found to be useful when specifying the OMCM:

- *The model is strictly ordered.* This is explicitly stated by Niessink and van Vliet and implied by Gartner. A strictly ordered model means that it is not possible to obtain a given level of maturity without first meeting the requirements of the previous levels. This reinforces the idea that organizations evolve the level of maturity over time instead of buying it all in one step.
- *The model is minimal.* Both models only state what is required to reach a given level. They do not restrict what might be done in addition to the minimum. The model also only describes what the requirements are—it does not specify how they are met.

Why A New Model?

The development of a capabilities model was driven by the need to provide a framework for the development and implementation of IT management infrastructure for Sun customers. Initially, we considered using one of the existing models (described previously) as the working model for operational capability. However, although there are advantages to using an available model, we encountered the following issues:

- A majority of the models are focused on process and deal very little with people or technology considerations. Because we have defined operational capability as the combination of people, process, and tools, it does not make sense to use a model that specified only the process component.
- A number of the available models were not defined at a level of detail that supported assessment or architecture efforts.
- These process models define maturity at any level as the existence or absence of specific processes. This true/false approach is inconsistent with our experience. Processes are implemented to various degrees within the organization over time, and that a capabilities model should describe this. The OMCM is an attempt to address these issues while taking advantage of existing work in the area.

What This Document Contains

This document provides a complete description of the OMCM, which includes both the components of operational capability (the Sun IT Management Framework) and the details of how this framework evolves over time.

This document consists of the following parts:

- Part 1, “Introduction,” consists of the following chapters:
  - Chapter 1, “Executive Summary”
  - Chapter 2, “Introduction”
- Part 2, “Sun IT Management Framework,” consists of the following chapters:
  - Chapter 3, “Sun IT Management Framework—Overview”
  - Chapter 4, “Sun IT Management Framework—People
  - Chapter 5, “Sun IT Management Framework —Process
  - Chapter 6, “Sun IT Management Framework—Tools
- Part 3, “Operations Management Capabilities Model (OMCM),” consists of the following chapters:
  - Chapter 7, “OMCM Specification—Overview”
  - Chapter 8, “OMCM Specification—People”
  - Chapter 9, “OMCM Specification—Process”
  - Chapter 10, “OMCM Specification—Tools”
- Part 4, “Conclusion,” consists of the following chapters:
  - Chapter 11, “Application of the OMCM”
  - Chapter 12, “Resources for More Information”
  - Chapter 13, “About the Authors”

1

Part 2—Sun IT Management Framework

Part 2 of this document describes the Sun IT Management Framework. Part 2 contains the following chapters:

- Chapter 3, “Sun IT Management Framework—Overview”
- Chapter 4, “Sun IT Management Framework—People
- Chapter 5, “Sun IT Management Framework —Process
- Chapter 6, “Sun IT Management Framework—Tools

3

Sun IT Management Framework—Overview

The OMCM needs to be specified within the context of a framework that allows us to quantify the components of operational capability. We call this framework the *Sun IT Management Framework* (or *Sun ITMF*.)

This chapter provides some context for the Sun IT Management Framework within the extended IT environment. It contains the following sections:

- Definitions of Key Terms
- Introduction to the Sun E-Stack
- Business Framework
- Execution Framework
- Sun IT Management Framework

The following three chapters provide additional detail on the Sun ITMF.

- Chapter 4, “Sun IT Management Framework—People”
- Chapter 5, “Sun IT Management Framework —Process”
- Chapter 6, “Sun IT Management Framework—Tools”

Definitions of Key Terms

Before describing the Sun IT Management Framework, we need to provide Sun's definitions for key terms—*system*, *framework*, *architecture*, and *design*—that are frequently ill defined and overused within the IT industry. Our working definitions apply within the context of this document—we do not make the claim that our definitions are the only correct ones.

Systems

Frameworks, architectures, and designs all provide a description of a *system*. In this document, a system is defined as *a group of elements that work cooperatively to provide specific results by performing specific tasks.*

System Development Steps

Most efforts to develop a system are *iterative* in nature, with each iteration focused on increasing levels of detail.

- The first step is to define the business requirements and priorities, quantify the problem to be solved, identify the major components of the solution, and make some general statements about their relationships. When possible, existing generalized descriptions of the problem and solution approaches are used.
- The next step is to add context to include the systemic qualities of the system (scalability, security, etc.) and the dependencies between the system and the environment within which it operates.
- The major components are further analyzed and developed. In many cases, the components may be treated as systems themselves that must be quantified and integrated with the other system components.
- Finally, the blueprint must be developed for the physical realization of the system that identifies the actual deployment approach within the environment.

Although these tasks provide is a very simplified description of systems development, the basic flow can be used to help provide definitions for framework, architecture, and design.

Framework, Architecture, and Design

The following table provides definitions used in this document for *framework*, *architecture*, and *design*.

TABLE 3-1 Definitions for Framework, Architecture, and Design

Term	Definition
framework	A predefined description of a system that helps identify all possible components of the system, and how they cooperate to provide the necessary functionality. This description is not developed within any context. A framework is primarily a starting point for systems development activities. It provides a mechanism for decomposing the system into a set of interrelated subsystems, each with their own components.
architecture	A system description that accounts for the constraints imposed by the environment within which the system will be used. An architecture is a system description with context. It is expressed at a level of detail that is sufficient to describe the technologies that will be used to realize it, to specify the integration methods between components, and to identify high risk elements of the solution that require further analysis.
design	A description of a system that details the physical realization of the architecture. A design provides the blueprint for the actual deployment of the system. It is specified at a level of detail that is sufficient to support project planning, development, acquisition, and provisioning activities.

The OMCM is specified within the context of the Sun IT Management Framework (Sun ITMF). We believe that the Sun ITMF conforms to the definition of framework as given above. Of course, actual system implementation requires additional effort. Defining an architecture or design of a management system is outside the scope of this document.

Introduction to the Sun E-Stack

To begin our description of the Sun ITMF, we need to describe how it fits into the overall IT environment. The following figure below is a representation of the IT environment that we refer to as the Sun *Enterprise Stack* (or *E-Stack*).

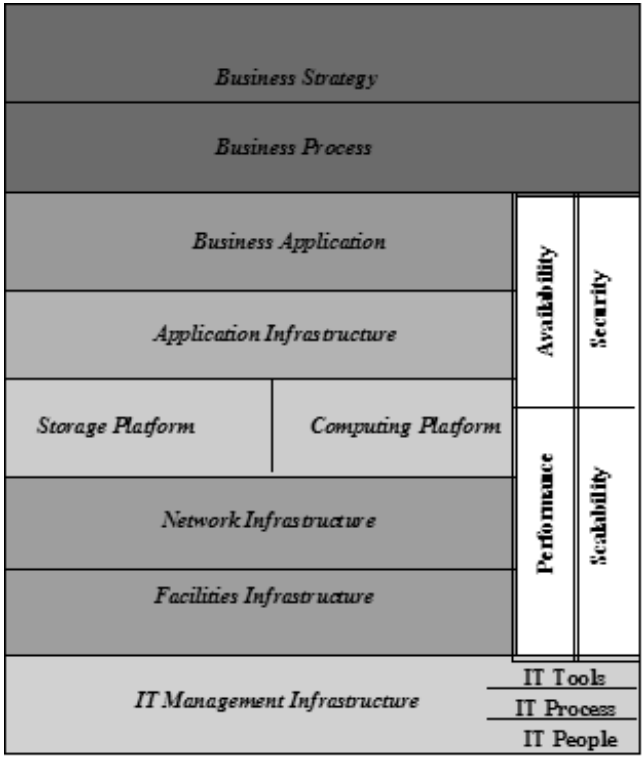

FIGURE 3-1 Sun Enterprise Stack (E-Stack)

The purpose of this construct is to visually describe all of the components and interactions that must be addressed when an organization delivers IT-based solutions to internal or external customers. Within any organization, the discipline of IT management is separate from, yet integrated with, the architecture that is managed. The process of developing an architecture is a complex, high-level set of tasks that considers the inputs, outputs, and dependencies of an IT service on the existing IT environment, along with the definition and mapping of requirements to technology. The E-Stack helps organize these considerations to ensure that they are addressed during the course of developing a solutions architecture.

A complete description of the various E-Stack layers is outside the scope of this document. However, the intent of each box is self evident and is defined later in this document, when the various frameworks that support the E-Stack are described.

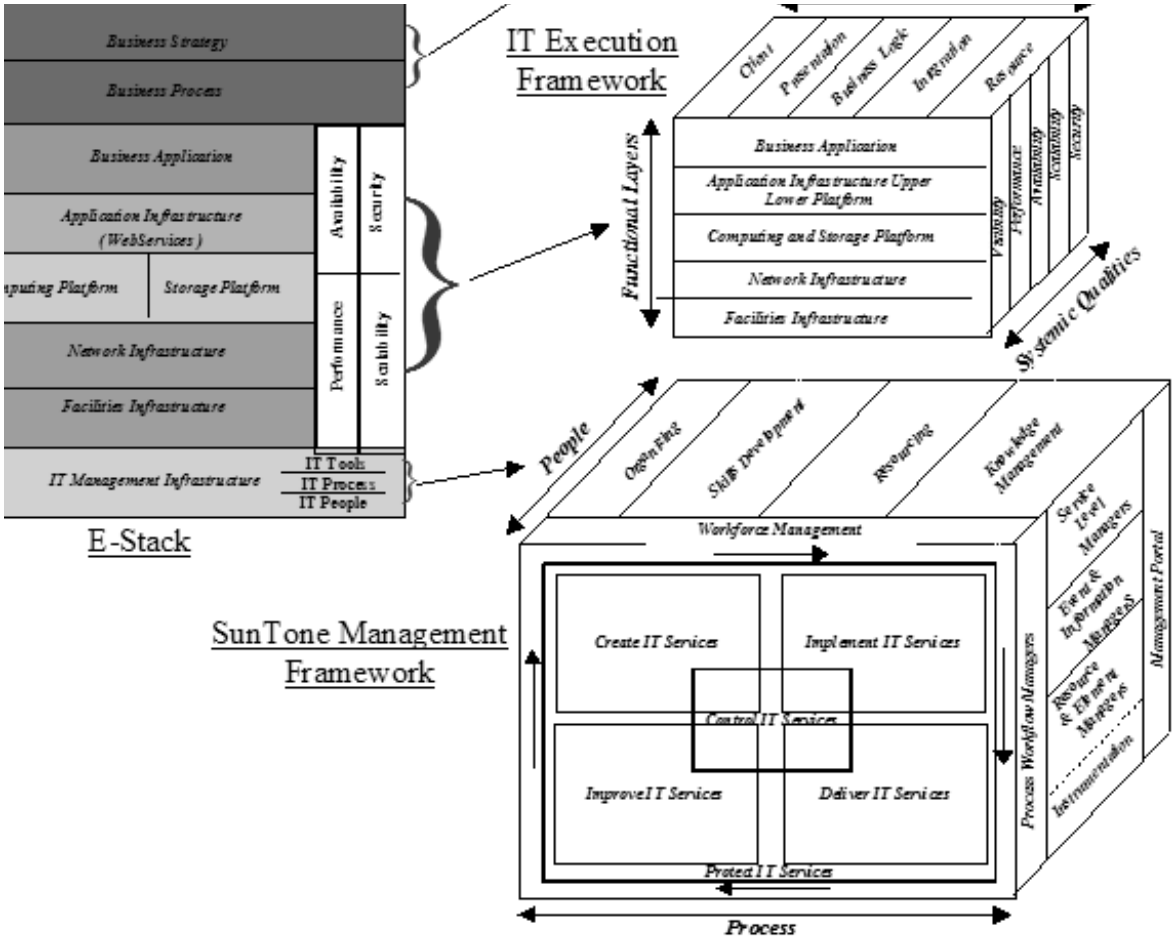

FIGURE 3-2 Three Core Frameworks Derived From the E-Stack

The components of the E-Stack involve three separate but mutually dependent architectural disciplines—the Business Framework, Execution Framework, and Sun IT Management Framework, as shown in the previous figure. The rest of this chapter describes these frameworks further.

Business Framework

The *Business Framework* encompasses the activities and requirements that drive the IT architecture process, as shown in the following figure.

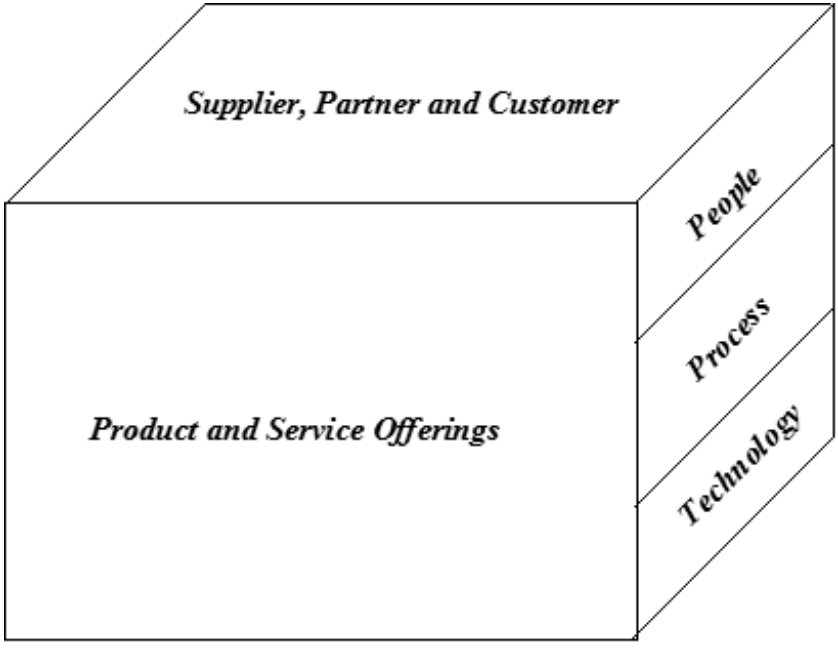

FIGURE 3-3 Business Framework

The Business Framework consists of:

- the various products and or services that are core to the organization's business
- the relationships with the organization's key external stakeholders (suppliers, partners, customers)
- the people, processes, and technology required to support the production and distribution of the organization's products and services.

The Business Framework provides the basis of the organization requirements for the Execution Framework and the Sun IT Management Framework.

Execution Framework

The *Execution Framework* encompasses the various application components (application, system hardware/software, network, etc.) and their supporting infrastructure.

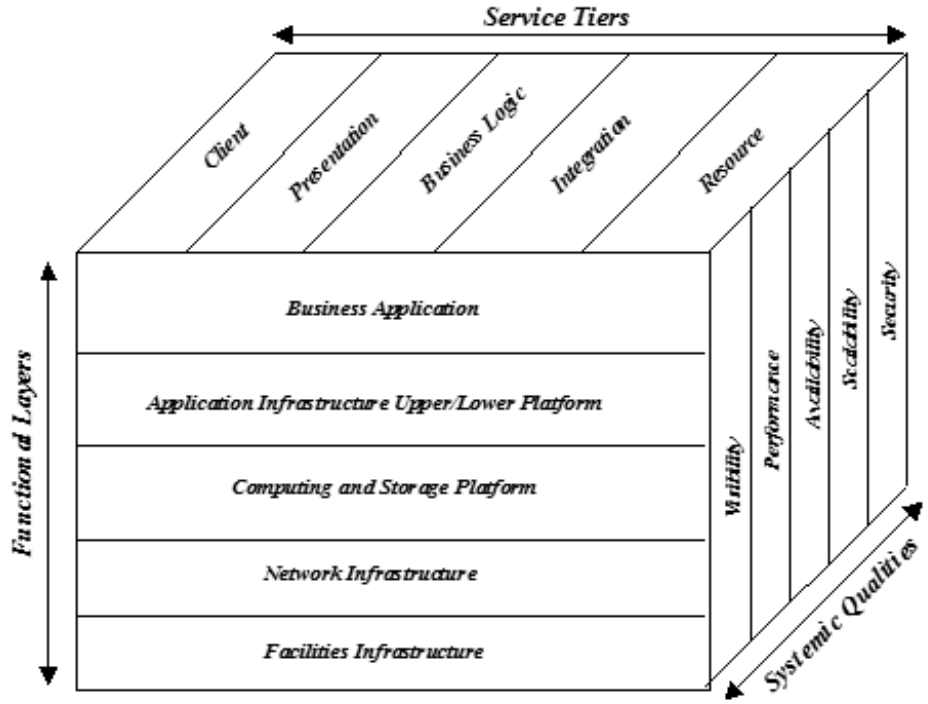

FIGURE 3-4 Execution Framework

Dimensions of the Execution Framework

This section describes the three dimensions of the Execution Framework—functional layers, service tiers, and systemic qualities.

Functional Layers

The *functional layers* of the Execution Framework describe the various technology components that make up an application, system, and the supporting environment, including:

- Business logic that captures the business process being implemented.
- Software container and services that this logic uses to execute its function.
- Supporting operating systems, hardware, and other components that provide computing and data storage.
- Network that connects the various distributed systems and enables communication.
- Facilities (power, heat, light, etc.) that provide the appropriate environment for all of the physical components of the architecture.

Service Tiers

The *service tiers* of the Execution Framework describe the logical partitioning of functions within a distributed application. References to "n-tier" applications are, in effect, describing this aspect of the Execution Framework.

Systemic Qualities

Systemic qualities capture the various non-functional (or operational) requirements that must be considered during the architectural process. These considerations do not impact *how* an application will work but rather *how well* it will work. Their position as the third aspect of the IT Execution Framework means that these requirements are considerations at each intersection of a service tier and functional layers.

Using the Execution Framework

The use of functional layers and service tiers helps to communicate and enforce common best practices of architecture development, such as the separation of concerns and the use of well defined interfaces. The result is a construct that allows the architect to decompose an application and to evaluate any one aspect, while keeping the other two aspects constant.

Special attention should be paid to the visibility component (systemic quality) of the Execution Framework. The degree to which this quality is considered and implemented will determine the amount of control over the Execution Framework that is provided to external entities represented by the management framework tools aspect.

Sun IT Management Framework

The following figure shows the Sun IT Management Framework (Sun ITMF).

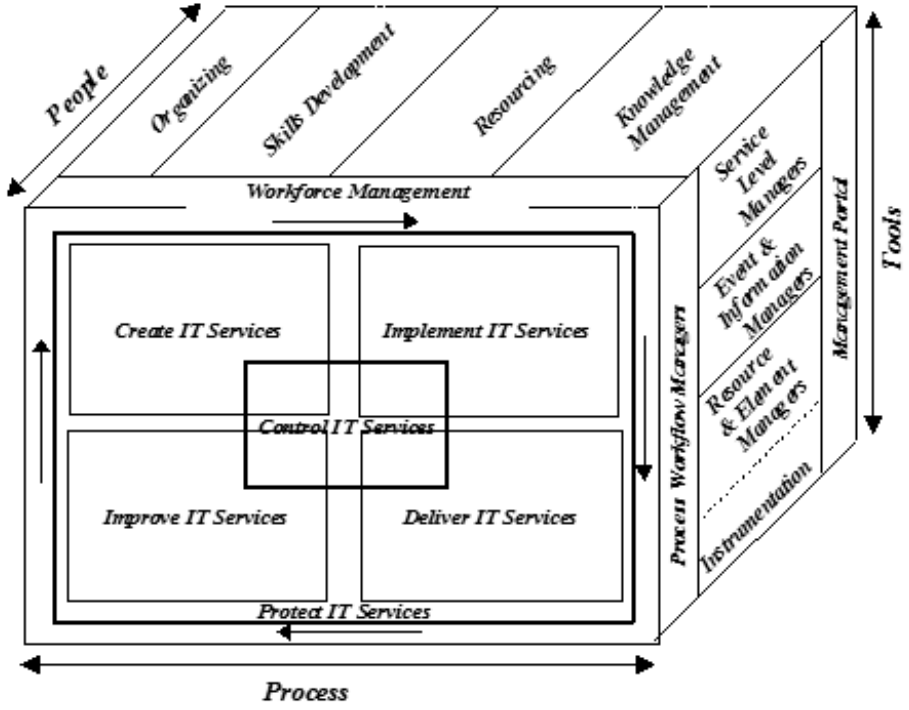

FIGURE 3-5 Sun IT Management Framework

Aspects of the Sun ITMF

The Sun ITMF consists of three different axes, or *aspects*, each of which details an important part of an organization's IT management infrastructure. These three aspects are what we have previously defined as the components of operational capability—people, processes, and tools.

The top-level description of each aspect is an abstraction of existing standards, such as the IT Infrastructure Library (ITIL®) or People Capability Maturity Model® (P-CMM®). Each aspect of the Sun ITMF is a generalized set of activities (people), processes (process), or functional categories (tools), under which specific solution approaches may be used. As will be seen in subsequent chapters, we have selected approaches that combine our interpretation of industry recognized standards and Sun best practices.

People Aspect

The *people aspect* of the Sun ITMF represents the *organizational component* of the IT environment. This includes IT operations staff, help desk organizations, operations and administrative groups, IT management, and any other internal IT stakeholders. The framework depicts a first level set of activities that are applied when managing IT staff. These activities are designed to cover a range of organizational management functions, such as designing the organization, obtaining resources, and managing resources on a day-to-day basis. This aspect also includes the concept of creating, capturing, and reusing organizational knowledge.

Process Aspect

The *process aspect* of the Sun ITMF represents the *actual IT management processes* that are needed to support the IT service life cycle. It describes processes for creating, deploying, and managing IT services.

Tools Aspect

The *tools aspect* of the Sun ITMF describes the *technology* used to facilitate and automate the execution of the various IT management processes. This framework is a functional categorization under which a variety of product approaches may be inserted.

Interaction Among the Aspects

FIGURE 2-1, "Components of Operational Capability," on page 5, shows the relationships among the three aspects of the Sun ITMF. For example, people can implement processes with or without tools—people might not need to use tools to implement a process. The nature of these relationships are not explicitly defined. However, architects and implementers should strive for a *loose coupling* of the aspects (no rigid rules on how these aspects interact) when the framework is being implemented in an organization.

As operational capability is being identified and the plan for improvement is developed, no one aspect (process, people, or tool) should invalidate or negate another. For example, a tool should not be drive the process so that a change in the tool would require a major rewrite of the process. In fact, the process should be defined first, the skills required next, and then the tool selected.

4

Sun IT Management Framework—People

This chapter describes the *people* aspect of the Sun IT Management Framework. It includes the following sections:

- Overview of the Sun ITMF People Aspect
- Practices of the Sun ITMF People Aspect
  - Organizing
  - Resourcing
  - Skills Development
  - Workforce Management
  - Knowledge Management

Overview of the Sun ITMF People Aspect

The *people aspect* of the Sun ITMF represents the organizational component of the IT environment. This includes IT operations staff, help desk organizations, operations and administrative groups, IT management, and any other internal IT stakeholders.

A major part of delivering IT services is managing the organizations that have responsibility for executing the various IT management processes. The *people aspect* of the Sun ITMF describes a set of practices necessary to ensure that the IT infrastructure is appropriately staffed with people who have the necessary skill sets. These activity groups also define practices necessary for the day-to-day management of the IT staff. The people aspect of the Sun ITMF describes a grouping of best practices for the development and management of an organization's IT workforce.

Diagram of the Sun ITMF People Aspect

The following figure shows the Sun ITMF People Aspect, its practice categories, and its specific practices.

Organizing	*Skills Development*	*Resourcing*	*Knowledge Management*
Workgroup Development	Career Development	Staffing	Competency Based
Participatory Culture	Training and	Competency Analysis	Assets
Empowered Workgroups	Development	Organizational	Continuous Workforce
Organizational	Competency	Capability Management	Innovation
Performance Alignment	Development	Continuous Capability	Competency Based
Competency Integration	Mentoring	Improvement	Practices
Workforce Planning			
Communication / Coordination			

Workforce Management

Work Environment	Compensation
Staff Performance Management	Quantitative Performance Management

FIGURE 4-1 Sun ITMF—People Aspect

The people aspect of the Sun ITMF is a process oriented improvement model. The IT organization can be matured through the institutionalization of different workforce management processes. The more integrated into the organization these processes become, the more effective and efficient the organization will be.

Practices and Practice Categories

The first level description of the people aspect (*practice category*) is a general categorization under which different best practices may be applied—organizing, skills development, resourcing, knowledge management, and workforce management. For the Sun ITMF, Sun modeled its practices on those defined in the Software Engineering Institute's People Capability Maturity Model (P-CMM)[7], although other suitable industry standard models could have been used instead. The following sections introduce each of the activity areas and their associated practices. For detailed descriptions of each practice, see Part 3, "OMCM Specification."

Definitions

This document makes frequent references to the notion of the *competency of the organization*. The term *competency*, along with other associated CMM terms, have very specific meanings within the CMM context. To clarify the use of CMM terminology in the context of the Sun ITMF, this section provides relevant definitions from the CMM reference.

Competency

Competency is an underlying characteristic of an individual that is causally related to effective/superior performance, as determined by measurable, objective criteria, in a job or situation. A correlation exists between an individual's competency and the effectiveness in performing their job.

Competency Based Practices

Competency based practices describe how individuals within a specific workforce competency apply their knowledge, perform their skills, and apply their process knowledge within the context of an organization's defined work processes. These practices might also include inter-process relationships (or multi-disciplinary processes).

An organization's defined processes are often described in terms of the processes and procedures related to different workforce competencies, such as the software development process, the sales process, or the customer training process. Competency-based processes and procedures are documented, trained, performed, enforced, measured, and improved over time. The competency-based processes

7. *People Capability Maturity Model P-CMM Version 2.0*, Bill Curtis, William E. Helfly, Sally A. Miller, Software Engineering Institute, July 2001.

associated with a single workforce competency might represent only part of a defined organizational process, because other elements of the defined process may be performed by individuals with different workforce competencies.

Competency Based Processes

Competency based processes define how individuals, within a specific workforce competency, apply their process knowledge and experience, and how they implement their skills, within the context of an organization's defined work processes.

Workforce Competency

Workforce competency is cluster of knowledge, skills, and process expertise that an individual should develop to perform a particular type of work in the organization. A workforce competency can be stated at a very abstract level, such as a need for a workforce competency in software engineering, financial accounting, or technical writing. Workforce competencies can also be decomposed into more granular abilities, such as competencies in designing avionics software, testing switching system software, managing accounts receivable, preparing consolidated corporate financial statements, or writing user manuals and training materials for reservation systems.

Practices of the Sun ITMF People Aspect

This section describes the practices associated with the Sun ITMF people aspect. Practices are grouped according to the following categories:

- Organizing
- Resourcing
- Skills Development
- Workforce Management
- Knowledge Management

Organizing

Organizing is the practice category that encompasses the activities related to the design of the organization's structure. These activities would include such practices as identifying organizational groups, developing specific roles and responsibilities for each group, and describing the interfaces between groups.

Organizing includes the following P-CMM practices:

- Communication / Coordination
- Workgroup Development
- Workforce Planning
- Participatory Culture
- Empowered Workgroups
- Competency Integration
- Organizational Performance Alignment

Communication / Coordination

Communication / coordination practices focus on the establishment and maintenance of information sharing within the organization. It includes the development of individual communications skills and the establishment of formal processes to ensure timely and effective two way communications.

Workgroup Development

A *workgroup* is a collection of individuals, managed by a single responsible individual, who work together on interrelated tasks in support of common goals. *Workgroup development* practices focus on identifying and creating these organizational groupings in support of specific objectives using a common, repeatable methodology.

Workforce Planning

Workforce planning practices focus on aligning the IT organization with the goals and objectives of the larger organization. This practice includes identifying the current and future competency needs of the organization based on expected activities, and then planning the steps necessary to acquire this capability when needed.

Participatory Culture

Participatory culture practices focus on ensuring that decision making is performed in a structured manner, and then is executed at the appropriate levels of the organization. The lines of communication established by the communication / coordination practice are used to ensure that work groups are informed about their performance and its impact on the overall performance of the company. The decision making process is designed to provide a balance of speed and effectiveness. Decision making is delegated to the levels in the organization that are best able to evaluate and implement the decisions.

Empowered Workgroups

Empowered workgroup practices involve workgroups that have responsibility and authority to determine how to most effectively conduct their operations. This practice is focused on the decentralization of planning, decision making, and operations to each workgroup. The workgroup is held accountable for their performance as measured against specific objectives.

Competency Integration

Competency integration practices refer to the integration of different workforce competencies to improve the efficiency of activities that have dependencies across areas of competency. The intent of this practice is to institutionalize the use of competency centers as building blocks to complete tasks requiring a multidisciplinary approach.

Organizational Performance Alignment

Organizational performance alignment practices focus on assessing what impact the aggregated performance of the various workgroups within the organization has on performance.

Resourcing

Resourcing is the practice category that encompasses the activities necessary to acquire the individuals necessary to meet the goals of the organization. This practice includes such activities as identifying required skill sets, determining how many of each type is required, developing a timeline for acquiring them, and identifying sources to fill the requirements.

Resourcing includes the following CMM practices:

- Staffing
- Competency Analysis
- Organizational Capability Management
- Continuous Capability Improvement

Staffing

Staffing practices involve matching work to individuals. This practice includes processes to recruit, select, and transition individuals into specific roles.

Competency Analysis

Competency analysis practices focus on analyzing the activities of the organization and developing the complete inventory of competencies needed to support them. This inventory includes the individual skills required as well as the identification of processes and knowledge necessary to meet the workforce requirements of the organization.

Organizational Capability Management

Organizational capability management practices focus on managing a workgroup's capability to perform the competency based processes that they use. This practice includes benchmarking the performance of the competency based processes by identifying key metrics, and then establishing the mechanisms to track and report on them.

Continuous Capability Improvement

C*ontinuous capability improvement* practices support workgroup efforts to continuously improve their performance of competency based practices. This practice includes processes to improve individual performance, workgroup operations, and cross competency coordination.

Skills Development

Skills development is a practice category that encompasses activities taken to help individuals acquire the knowledge and practical abilities necessary to perform their current job or to prepare them for future assignments. Skills development includes the following CMM practices.

- Training and Development
- Career Development
- Competency Development
- Mentoring

Training and Development

The purpose of *training and development* practices is to close the gaps between individual skills and the requirements of their current position. This practices include steps taken to provide individuals with opportunities to develop new skills in anticipation of future needs.

Career Development

Career development practices assist individuals with meeting their career goals and objectives. This practice involves defining development paths that identify the requirements for advancement, and communicating these development paths to the organization. Periodic reviews of career aspirations and opportunities are performed with individuals to ensure that they understand the options available within the organization. The goal is to ensure that individuals see the organization as a place where they can develop and realize individual career goals.

Competency Development

Competency development practices focus on continuously improving the ability of the workforce to execute the required competency based processes.

Mentoring

Mentoring practices involve facilitating the transmission of experience and knowledge throughout the organization. This process is normally performed by individuals as they pass on their competency knowledge to others via formal and informal relationships.

Workforce Management

Workforce management is a practice category that encompasses the activities performed to control and support individuals as they perform their tasks. Workforce management includes the management of individual performance and compensation, as well as the activities necessary to provide the workforce with the infrastructure required to perform their job functions.

Workforce management includes the following CMM practices:

- Work Environment
- Staff Performance Management
- Compensation
- Quantitative Performance Management

Work Environment

Work environment practices involve ensuring that the physical working environment is conducive for individuals to perform their job functions in an effective and efficient manner. This practice includes the development of processes to evaluate and maintain the physical environment (work space), supporting technology (computers, phones, etc.), procedures to minimize distractions, and so on.

Staff Performance Management

Staff performance management practices involve identifying metrics against which individual and workgroup performance can be measured. The intent is to facilitate continuous discussion on individual and workgroup performance with the purpose of identifying ways to improve this performance. The goal of staff performance management is the creation of a feedback loop within which performance is measured, evaluated, and improved. Mechanisms for rewarding superior performance are identified and formalized in order to reinforce the appropriate behaviors.

Compensation

Compensation practices involve providing financial rewards to individuals in proportion to their contributions to the organization. The goal is to provide a system that is viewed within the organization as equitable. Once an equitable reward system is in place, it can be used to motivate and reinforce specific behaviors that are deemed important to achieving the goals of the organization.

Quantitative Performance Management

Quantitative performance management practices focus on the continuous performance improvement of critical competency based processes. This practice involves identifying the priority processes, developing metrics that are descriptive of the effectiveness and efficiency of these processes, and then applying a process improvement methodology to improve performance. Within Sun, the Sun^{SM} Sigma methodology is used as the basis of process improvement activities.

Knowledge Management

Knowledge management is a practice category that encompasses such activities as the capture, documentation, maintenance, and dissemination of organizational learning. Knowledge management enables the creation and maintenance of competency-based practices. Through the execution of knowledge management, organizations are able to take successful solutions and institutionalize them for reuse. It is through this set of practices that organizations distribute effective processes and make them repeatable.

Knowledge management includes the following CMM practices:

- Competency-Based Practices
- Competency-Based Assets
- Continuous Workforce Innovation

Competency-Based Practices

Competency-based practices are focused on the development of workforce competencies. These practices are used to align the staffing, compensation and other resourcing practices with the competency development goals of the organization.

Competency-Based Assets

The purpose of the *competency-based assets* practices is to capture the lessons learned and artifacts developed during the execution of competency-based processes. Workforce competency is expanded beyond the skills of the individual workers and larger organizational units to include the reusable processes and other assets of the company. These practices include the activities necessary to capture knowledge, as well as the mechanisms used to disseminate this knowledge throughout the organization so that it becomes an integral part of the organization.

Continuous Workforce Innovation

Continuous workforce innovation practices focus on continuous improvement efforts for the workforce. This practice includes the activities involved with setting policies for workforce improvement, measuring the performance of the organization against the goals, and facilitating workforce process improvement through the identification of opportunities and the implementation of new approaches.

5

Sun IT Management Framework — Process

This chapter describes the *process* aspect of the Sun IT Management Framework. It includes the following sections:

- Overview of the Sun ITMF Process Aspect
- Processes of the Sun ITMF Process Aspect
  - Implement IT Services
  - Deliver IT Services
  - Improve IT Services
  - Control IT Services
  - Protect IT Services

Overview of the Sun ITMF Process Aspect

The *process aspect* of the Sun ITMF represents the actual IT management processes that are needed to support the IT service life cycle. The process aspect describes processes for creating, deploying, and managing IT services.

Diagram of the Sun ITMF Process Aspect

The following figure shows the Sun ITMF people aspect, its process categories, its specific processes, and the relationships among them:

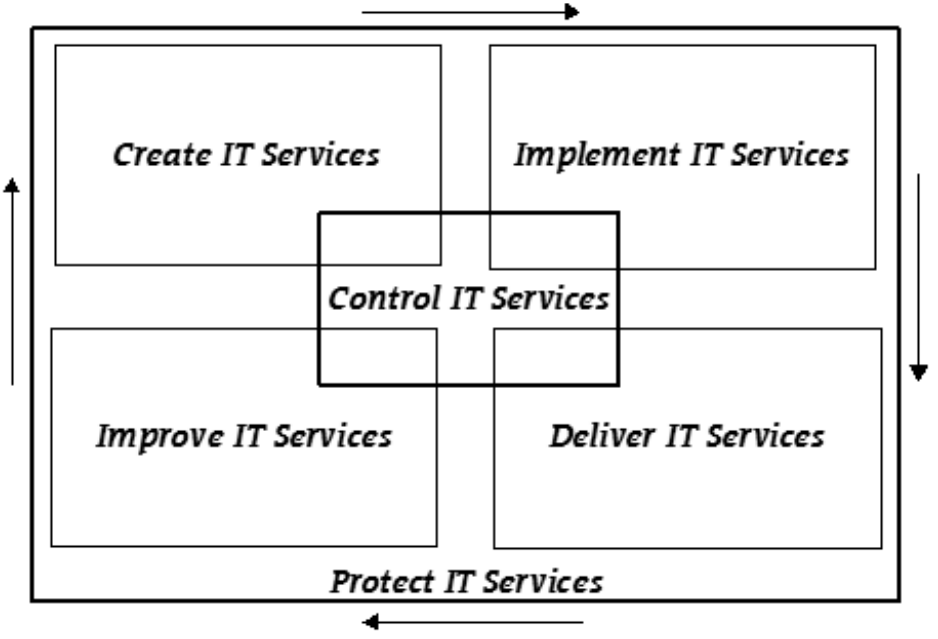

FIGURE 5-1 Sun ITMF—Process Aspect

Processes and Process Categories

The process categories of the Sun ITMF have been organized in several major components. Each component describes the key activities that must occur in the datacenter to assure proper levels of IT service.

The rationale behind these process categories is based on two notions:

- IT services have a life cycle, and this should be reflected in the processes.
- Each category requires specific and different skill sets and mind-set.

  When creating services, organizations need people that can think out of the box with a business focus. Implementing IT services means a focus on meeting schedules and resource challenges. The deliver IT service process category brings the focus to consistent service quality. The improve IT service process category requires a focus on understanding how to measure and a how to facilitate process improvement. Both the control and protect process categories have aspects that require a look beyond the IT environment into other areas, such as finance, security, and business continuity.

Sun ITMF process categories are designed to allow for the easy mapping of different IT standards. In this document, we include process standards as they are defined in the Information Technology Infrastructure Library (ITIL) to provide us with the details to determine the degree of implementation of a process. The categorization of these processes is based on a center of gravity approach, meaning that it is widely recognized that most activities, as defined by ITIL, revolve around the target category but that certain aspects can, and most likely will, also play in different categories. For more information about ITIL, see www.itil.co.uk/.

IT Services

In this document, a *IT service* is defined as the end-to-end provision of the people, process, and technology necessary to deliver a specific organization requirement. It includes all of the activities and components required to deliver a service, through IT, to the end user.

Processes of the Sun ITMF Process Aspect

This section describes the processes associated with the Sun ITMF process aspect. Processes are grouped according to the following categories:

- Implement IT Services
- Deliver IT Services
- Improve IT Services
- Control IT Services
- Protect IT Services

Create IT Services

The *create IT services* process category describes all processes related to the creation of new services, including identifying, quantifying, architecting, and designing IT services. It involves:

- Determining what services are needed and desired for the IT customers.
- Defining of the relationship between IT customers and the IT service provider, including the definition of Service Level Agreements (SLAs).
- Addressing the processes that ensure the completeness of the IT service portfolio and the alignment of the IT Services with each other.

Create IT services includes the following ITIL based processes:

- Service Level Management
- Availability Management

Service Level Management

The *service level management* (SLM) process involves:

- planning, coordinating, drafting, agreeing, monitoring, and reporting on SLAs
- the on-going review of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved.

SLAs provide the basis for managing the relationship between the provider and the IT customer. An SLA is a written agreement between the IT service provider and the IT service customer(s). It defines the key service targets and responsibilities of both parties. The emphasis must be on *agreement*—SLAs should not be used for coercing one side or the other. A true *partnership* should be developed between the IT

provider and the customer so that a mutually beneficial agreement is reached; otherwise, the SLA could quickly fall into disrepute and an ensuing culture of blame could prevent the development of any true service quality improvements.

The following figure illustrates the SLM process:

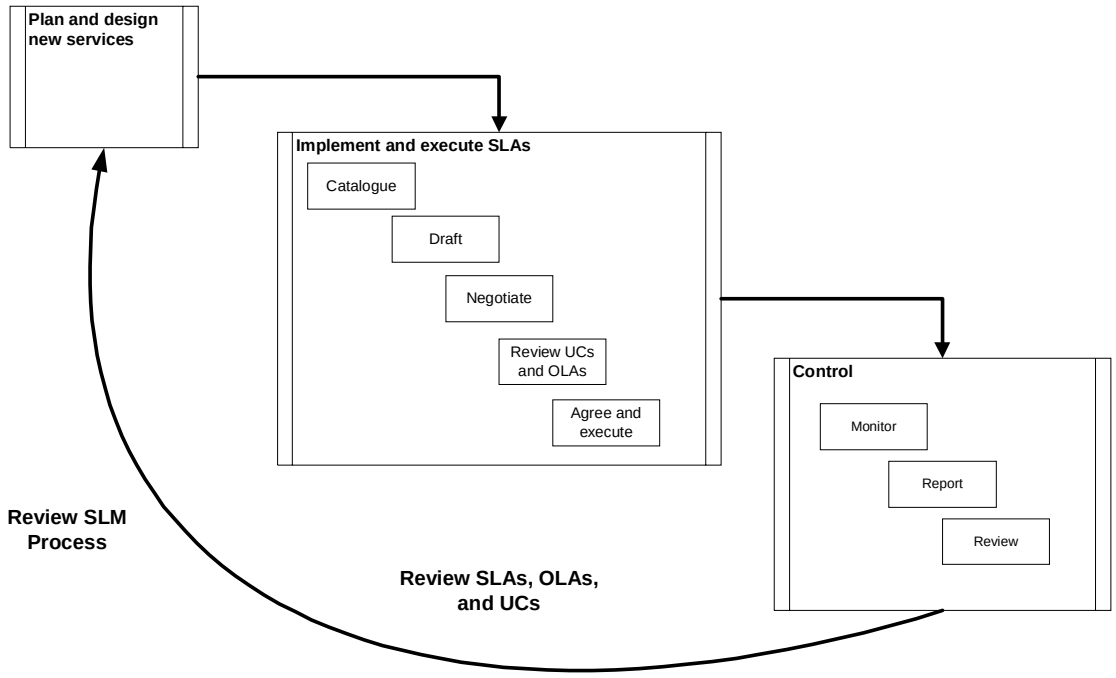

FIGURE 5-2 Service Level Management Process

The service level management process includes the following main categories of activities (note that this is a circular process):

- plan and design
- implement and execute
- control and feedback

Availability Management

The *availability management* process involves managing key components of the predictability and availability of IT services. Availability requirements heavily influence service architecture design. Availability management is the process that assures the ability of an IT service or component to perform its required function at a stated instant or over a stated period of time.

Availability (or, rather, unavailability) is the key indicator of service quality perceived by business users. Availability is underpinned by the reliability and maintainability of the IT infrastructure and the effectiveness of the IT support organization. An IT service that consistently meets its SLA's availability targets has the characteristics of low frequency of failure and rapid resumption of service after an incident has occurred.

The following figure shows the inputs and outputs of the availability management process, as well as the importance of being driven by business requirements.

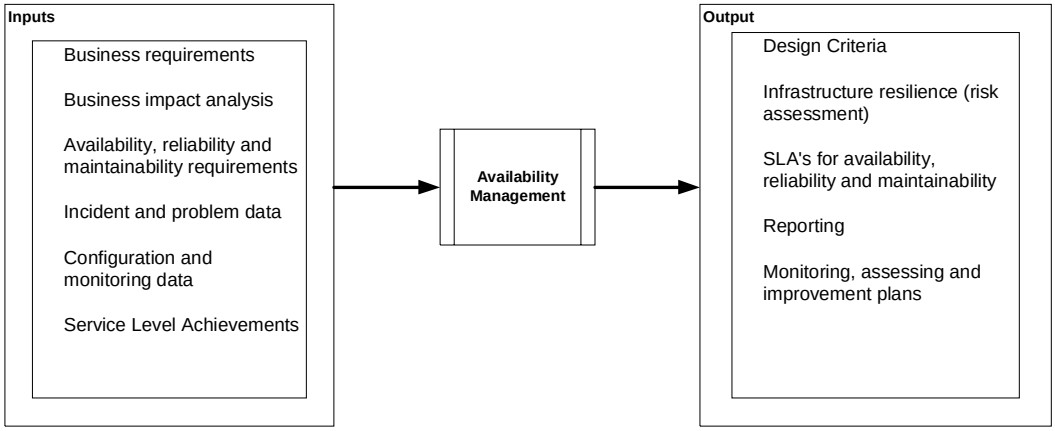

FIGURE 5-3 Availability Management Process—Inputs and Outputs

Availability depends on other components of the service. The following figure shows what these relationships are and how they are managed.

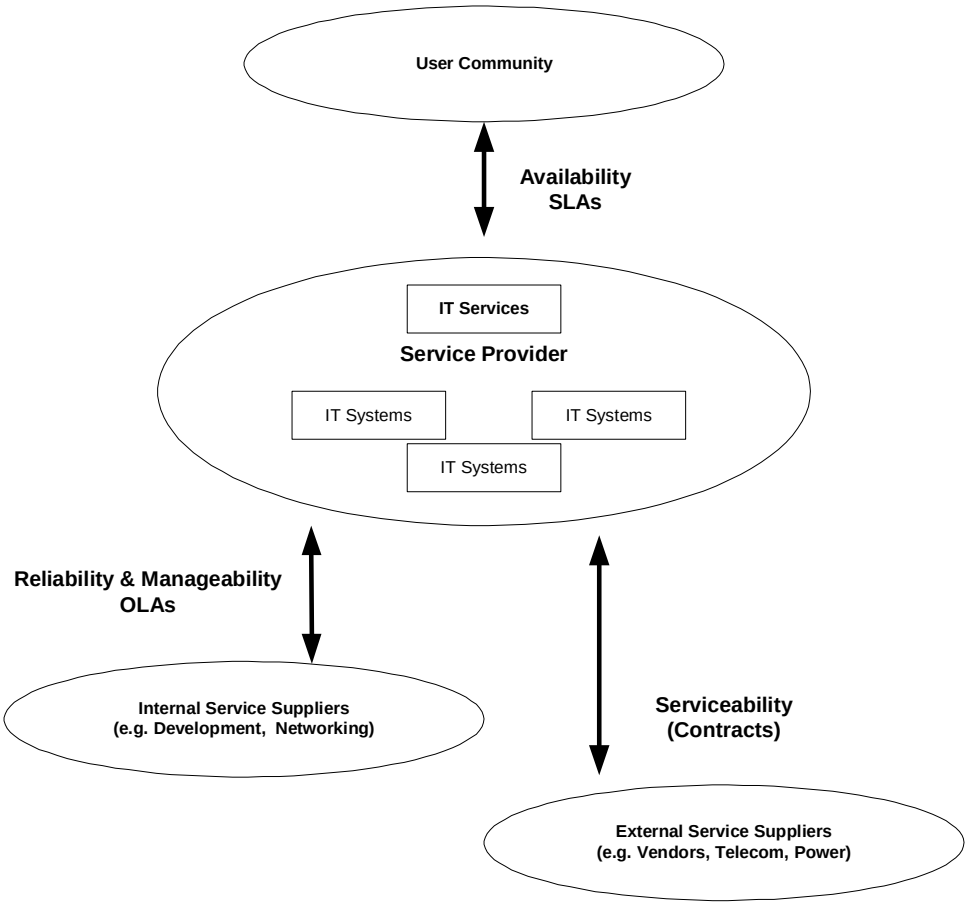

FIGURE 5-4 Availability Management Process—Dependencies and Contracts

This figure also shows the terminology and type of contracts used to define the relationships. Additional details about the structure of these agreements are outside the scope of this document.

Implement IT Services

The *implement IT services* process category encompasses efforts to properly roll-out of a new or updated IT service that has been created. Implement IT services includes the ITIL based Release Management process.

Release Management

The *release management* process involves a collection of authorized changes to an IT service. A release typically consists of a number of problem fixes and enhancements to the service, the new or changed software required, and any new or changed hardware needed to implement the approved changes. The following table describes the most common categories of releases:

TABLE 5-1 Release Management Categories

Release Category	Description
Major software releases and hardware upgrades	Normally contain large areas of new functionality, some of which may make intervening fixes to problems redundant. A major upgrade or release usually supersedes all preceding minor upgrades, releases, and emergency fixes.
Minor software releases and hardware upgrades	Normally contain small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
Emergency software and hardware fixes	Normally contain the corrections to a small number of known problems.

Release management is concerned with changes to defined IT services. The release management process facilitates the following activities involved in the implementation of IT Services:

- Planning and overseeing the successful rollout of software and related hardware.
- Designing and implementing efficient procedures for the distribution and installation of changes to IT systems.
- Ensuring that the hardware and software being changed is traceable, secure, and that only correct, authorized, and tested versions are installed
- Communicating with, and managing the expectations of, the customer during the planning and rollout of new releases.
- Achieving agreement about the exact content and rollout plan for the release through liaison with change management.

- Implementing new software releases or hardware into the operational environment using the controlling processes of configuration management and change management. A release should be under change management and may consist of any combination of hardware, software, firmware, and documentation configuration items.
- Ensuring that master copies of all software are secured in the definitive software library (DSL) and that the Configuration Management Data base (CMDB) is updated.
- Ensuring that all hardware being rolled out or changed is secure and traceable, using the services of configuration management.

The focus of release management is the protection of the live environment, or IT service delivery environment, and its services through the use of formal procedures and checks.

Release management works closely with the change management and configuration management processes to ensure that the shared CMDB is kept up-to-date following changes implemented by new releases, and that the content of those releases is stored in the DSL. Hardware specifications, assembly instructions, and network configurations are also stored in the DSL/CMDB.

The following figure shows the main release activities and its close ties to configuration management.

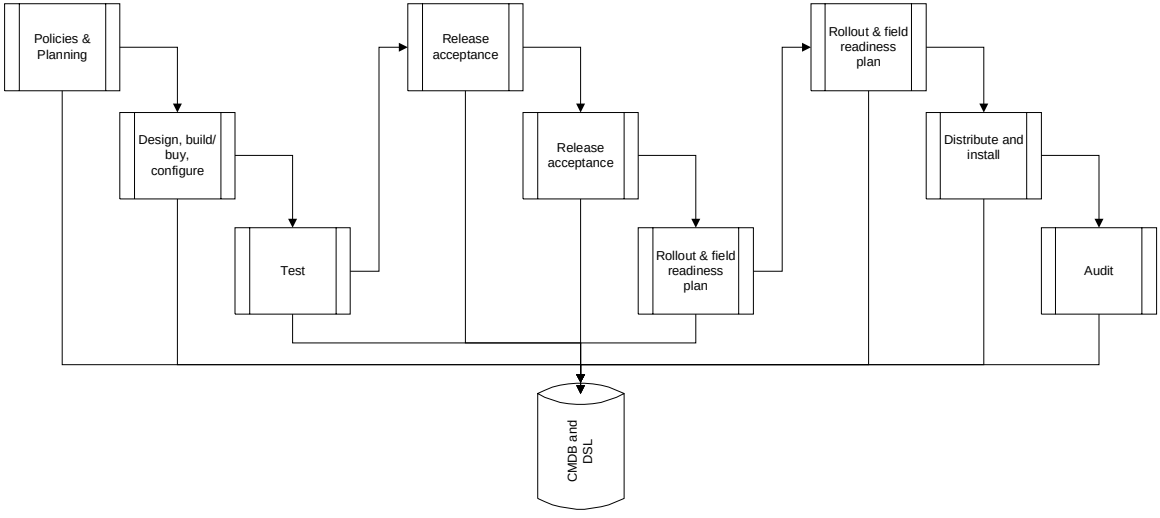

FIGURE 5-5 Release Management Activities

Deliver IT Services

The *deliver IT services* process category is the most visible part of the IT organization's activities. This category addresses all activities that assure the proper delivery and ongoing operation of the IT services, including efforts to assure predictable, consistent service delivery. This is often referred to as *IT operations* or *data center operations*.

Deliver IT services includes the following ITIL based processes:

- Capacity Management
- Incident Management
- Service Desk

Capacity Management

The *capacity management* process involves ensuring that the capacity of the IT infrastructure matches the evolving demands of the organization in the most cost-effective and timely manner. The process encompasses:

- Monitoring performance and throughput for IT services and the supporting infrastructure components.
- Tuning system components to make the most efficient use of existing resources.
- Understanding the demands currently being made for IT resources and producing forecasts for future requirements.
- Influencing the demand for resources, perhaps in conjunction with financial management.
- Producing a capacity plan that enables the IT service provider to deliver services of the quality defined in the SLAs.

Capacity management is essentially a balancing act—balancing cost against capacity to ensure that:

- purchased processing capacity is cost justifiable in terms of organization need
- priority is given to making the most efficient use of resources
- supply meets demand—the available supply of processing power matches the demands made on it by the organization, both now and in the future; it may also be necessary to manage or influence the demand for a particular resource.

The following figure illustrates the key inputs and outputs of capacity management.

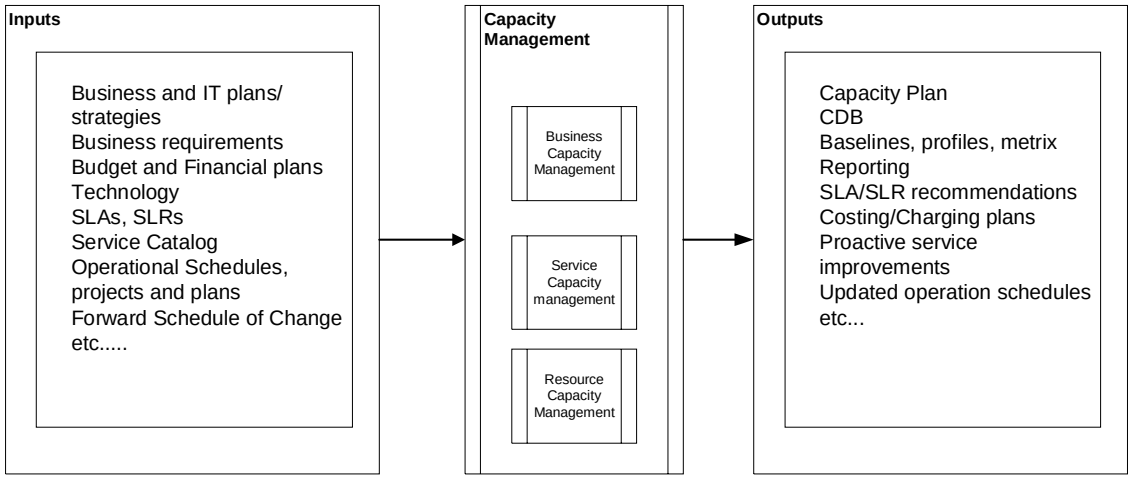

FIGURE 5-6 Capacity Management Process—Inputs/Outputs

Capacity planning occurs at the following three different levels.

TABLE 5-2 Capacity Planning Levels

Level	Description
Business Capacity Management	Trends, forecasts, models, and documents future business requirements.
Service Capacity Management	Monitors, analyzes, tunes, and reports on service performance. Establishes baselines and profiles the use of services and manages the demand for services.
Resource Capacity Management	Monitors, analyzes. and reports on the utilization of IT components to establish baselines and profiles of use of components.

The capacity planning process should include the fact that all three levels influence each other.

Incident Management

The *incident management* process involves activities associated with service disruptions. The primary goal of the incident management process is to restore normal service operation as quickly as possible, minimizing the adverse impact on business operations and ensuring that the best possible levels of service quality and availability are maintained. Normal service operation means that services are

delivered within the SLA limits. Incident management is closely related with the problem management process that looks to find the root cause for multiple similar incidents and has a clear goal of improving, amongst other things, service reliability.

The following figure shows the key activities of incident management and its relationships with other process components, including configuration management, problem management, and change management.

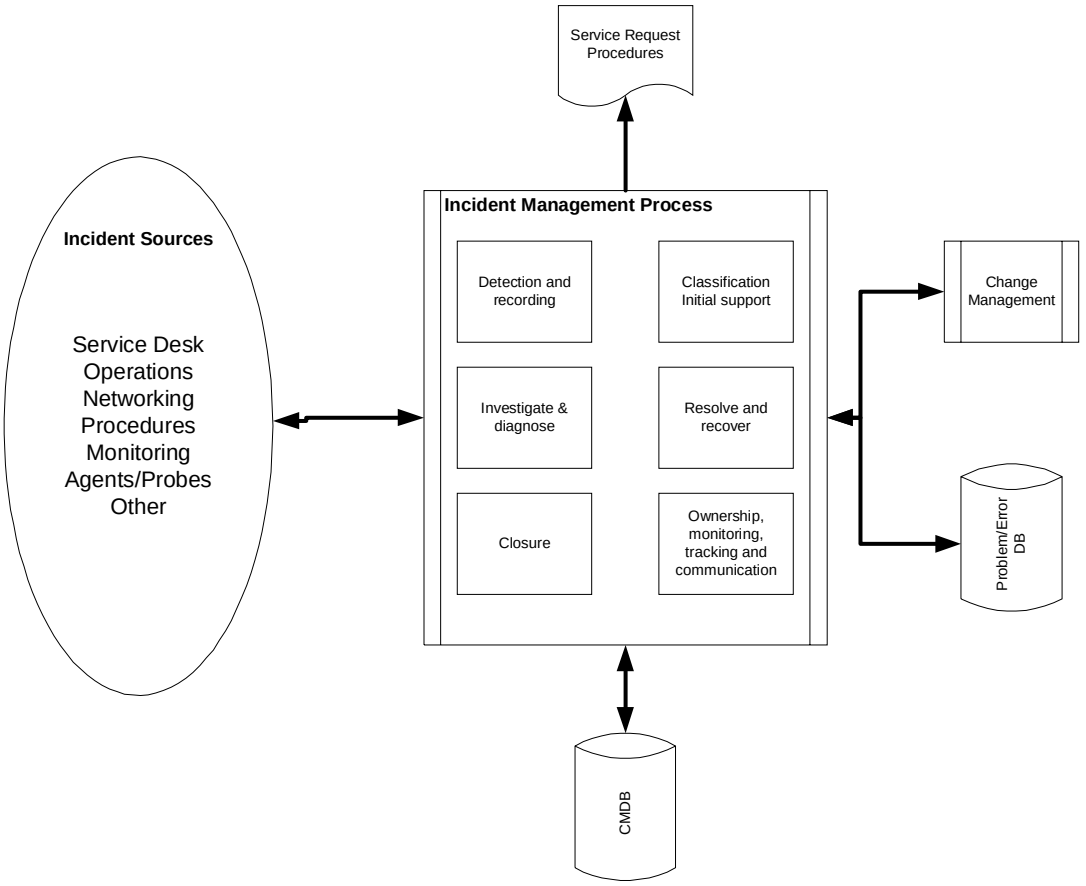

FIGURE 5-7 Incident Management Process

Service Desk

The *service desk* process involves a central point of contact for handling customer, user, and related issues to meet customer and business objectives. This function is known under several possible names (or their variants), including:

- Service Desk

- Help Desk
- Call Center
- Customer Hot line

The service desk extends the range of services and offers a more global-focused approach, allowing business processes to be integrated into the service management infrastructure. It handles incidents, problems, and questions. The service desk also provides an interface for other activities, such as customer change requests, maintenance contracts, software licenses, service level management, and configuration management, availability management, financial management for IT services, and IT service continuity management.

The service desk is customer-facing and its main objectives are to drive and improve service to—and on behalf of—the organization. At an operational level, its objective is to provide a single point of contact that dispenses advice, guidance, and the rapid restoration of normal services to its customers and users.

The roles and responsibilities of the service desk are dependent on the nature of the organization's business and of the support infrastructure in place. For most organizations, a primary role is the recording and management of all incidents that affect the operational service delivered.

As a single point of contact, it is important that the service desk minimally provide the customer with a status update on service availability and any request being managed by the service team, including the incident number for use in future communication. Status update information can include:

- Likely request completion time
- When their equipment move or installation is scheduled for
- When a new release is planned
- Status on service enhancements
- Where to get further information on a subject
- Whether the computer systems are available at a given time

Common service desk functions include:

- Receiving calls, first-line customer liaison
- Recording and tracking incidents and complaints
- Keeping customers informed on request status and progress
- Making an initial assessment of requests, attempting to resolve them or referring them to someone who can, based on agreed service levels
- Monitoring and escalation procedures relative to the appropriate SLA
- Managing the request life-cycle, including closure and verification
- Communicating planned and short-term changes of service levels to customers
- Coordinating second-line and third-party support groups
- Providing management information and recommendations for service improvement
- Identifying problems
- Highlighting customer training and education needs

- Closing incidents and confirmation with the customer
- Contributing to identification

The key benefit to having a service desk lies in the communication it provides between service customers and the support teams—providing customers with information so they are being helped. The service desk communicates the status, while the support organization focuses on doing the work to fix the problem or otherwise fulfill requests.

Improve IT Services

The *improve IT services* process category addresses all activities surrounding the measurement and optimization of IT service activities with the goal of continuously improving service levels.

ITIL has included many of these components in each process, but problem management is the focal point for root cause analysis and the prevention of issues. Sun has developed Sun^{SM} Sigma to formalize a methodology to facilitate process improvement—in general and specifically in the IT environment. In combination, problem management and continuous process improvement (Sun Sigma) create a solid foundation to facilitate continuous service level improvement.

Improve IT services includes the following ITIL based processes:
- Problem Management
- Continuous Process Improvement

Problem Management

The *problem management* process involves:

- minimizing the adverse impact of incidents and problems on the organization that are caused by errors within the IT infrastructure
- preventing the recurrence of incidents related to these errors

In order to achieve this goal, problem management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation.

The problem management process has both reactive and proactive aspects.

- *Reactive problem management* is concerned with solving problems in response to one or more incidents.
- *Proactive problem management* is concerned with identifying and solving problems and Known errors before incidents occur in the first place.

The focus of the problem management process is to reduce both the number and severity of incidents and problems. Therefore, a key component of problem management is to ensure that previous information is documented in such a way that it is readily accessible to the service desk function. In addition, problem management involves:

- Making sure that the information is indexed so that it is easily referenced as part of identifying new incidents.
- Continuous updates due to changes in:
  - technology
  - available external solutions
  - business practices and requirements
  - available skills
  - frequency and impact of recurring incidents
  - interpretation of internal best practice
- The process is subject to a detailed review.
- Training of staff and their feedback.
- Automation to maintain the repository.

Problems and known errors can be identified by:

- Analyzing incidents as they occur (reactive problem management).
- Analyzing incidents over differing time periods (proactive problem management).
- Analyzing the IT infrastructure
- Providing a knowledge database.
- Developers / vendors when new products are introduced.

A *problem* is a condition that is often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown but for which the impact is significant. A *known* error is a condition identified by successful diagnosis of the root cause of a problem, and the subsequent development of a work-around.

Continuous Process Improvement

Although ITIL understands the need for *continuous process improvement*, it has not defined a separate discipline to address this important aspect. The Sun ITMF uses the processes as defined by Sun internally. However, any approach based on Sun[SM] Sigma—or any Sigma-based approach, for that matter—should provide sufficient rigor and commitment to sufficiently address this area.

Sun Sigma is the core methodology that Sun is using to achieve industry-leading availability and quality. Sun Sigma drives key processes with data about critical customer requirements. *Sigma* is the term used in statistical analysis for variation

from perfection. Sun attains a common measurement of quality for any type of process by using data to define and control process, and then measuring defects across a project (or across the organization).

Sun Sigma refers to a methodology commonly known as Six Sigma (see http://www.isixsigma.com/). The objective of Sun Sigma is to completely satisfy customer requirements profitably. We call it Sun Sigma because not all customers will require all of the processes to yield products or services at 6 sigma (such as 3.4 defects per million opportunities, or *DPMO*). The real challenge is to more thoroughly understand customer requirements and plan the sigma levels of the products, services, and processes accordingly.

Control IT Services

The *control IT services* process category involves ensuring that IT services are delivered within the constraints identified by the governing body and includes the processes that facilitate the governing activities. Examples of governing functions are: financial controls, audit, alignment with organizational objectives, and so on.

The control process category includes the following ITIL based processes:

- IT Financial Management
- Configuration Management
- Change Management

IT Financial Management

The *IT financial management* process involves controlling the monetary aspects of the organization. It supports the organization in planning and executing its business objectives and requires consistent application throughout the organization to achieve maximum efficiency and minimum conflict.

Within an IT organization, IT financial management it is visible in three main processes:

TABLE 5-3 IT Financial Management Processes

Process	Description
budgeting	Process of predicting and controlling the spending of money within the organization. Consists of periodic negotiation cycles to set budgets (usually annual) and the day-to-day monitoring of current budgets
IT accounting	Set of processes that enable the IT organization to account fully for the way its money is spent (particularly the ability to identify costs by customer, by service, am by activity). It usually involves ledgers and should be overseen by trained accountants.
charging	Set of processes required to bill customers for the services that the organization supplies to them. This requires sound IT accounting to a level of detail determined by the requirements of the analysis, billing, and reporting processes.

The following figure illustrates the Financial Management Cycle.

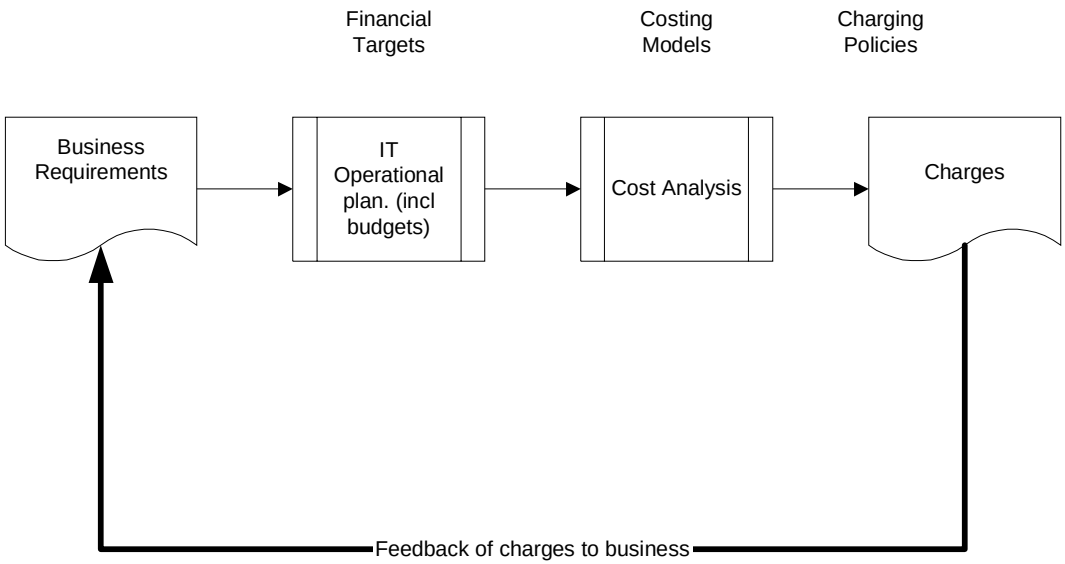

FIGURE 5-8 Financial Management Cycle

In this diagram, it is assumed that charging for IT services might be desirable. This could be considered by large IT service providers, such as Internet Service Providers (ISPs), but the process of charging become less effective for smaller organizations. IT must be able to justify its cost in relation to the business objectives at any time. IT financial management sets out to provide that capability.

Configuration Management

The *configuration management* process provides a logical model of the infrastructure or a service by identifying, controlling, maintaining, and verifying the versions of configuration items (CIs) in the organization.

The goals of configuration management are to:

- Account for all IT assets and configurations within the organization and its services.
- Provide accurate information on configurations and their documentation to support all the other service management processes.
- Provide a sound basis for incident management, problem management, change management, and release management.
- Verify the configuration records against the infrastructure and correct any exceptions.

Configuration management can be considered the glue between most processes because it provides and maintains all vital information about IT service implementations. As a result, configuration management is tightly integrated with incident management, problem management, release management, and change management, as shown in the following figure.

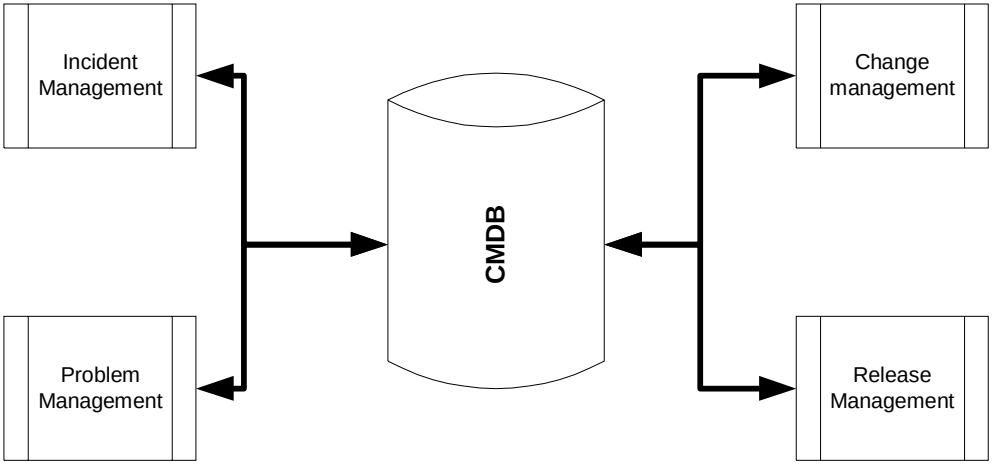

FIGURE 5-9 Configuration Management Database

Change Management

The *change management* process involves ensuring that standardized methods and procedures are used for efficient and prompt handling of all changes, with the goal of minimizing the impact of change-related incidents upon service quality and, consequently, to improve the day-to-day service delivery of the IT organization.

Making an appropriate response to a change request entails a considered approach to risk assessment and business continuity, change impact, resource requirements, and change approval. This considered approach is essential to maintain a proper balance between the *need* for change and the *impact* of the change.

Note that change management processes need to have high visibility and open channels of communication in order to promote smooth transitions while changes are occurring.

The basic thrust of change management is mainly process-related and managerial, rather than technical. In contrast, incident management is primarily technical, with a strong emphasis on the mechanical nature of some of the processes.

Change management is responsible for managing its interfaces with other business and IT functions. The following figure shows a sample process model of change management. This is just one example—the way in which an organization decides to implement the change management process is, to a large extent, driven by the available resources (time, priorities, people, and budget).

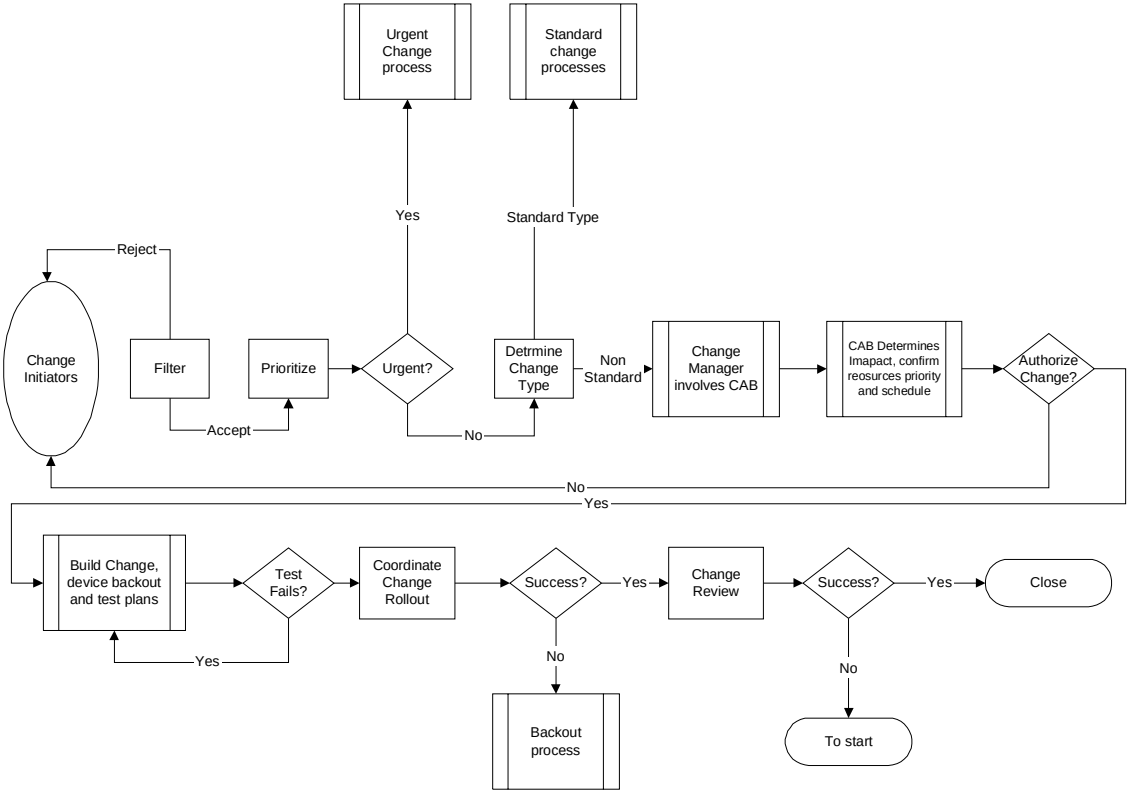

FIGURE 5-10 Change Management Process

In this figure, a standard change process is shown as a separate activity. As IT organizations mature, the change management process increasingly enables speedier deployment of changes with limited impact and/or risk. Change management defines common or well known changes and, therefore, can allow for a more streamlined implementation process.

Protect IT Services

The *protect IT services* process category involves ensuring that IT services are still available under extraordinary conditions, such as catastrophic failures, security breaches, unexpected heavy loads, and so on. This area has become increasingly important as organizations depend more and more on IT services. Therefore, implementing IT service protection at the right levels is crucial to an organization's strength and survival.

Protection includes the following ITIL based processes:

- IT Service Continuity Management
- Security Management

IT Service Continuity Management

The *IT service continuity management* (*ITSCM*) process supports the overall business continuity management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support, and service desk) can be recovered within required and agreed upon business time constraints.

IT service continuity has become critical to an organizational survival as organizations have become increasingly dependent upon technology. Technology is a core component of most business processes.

Continuity is bolstered by implementing risk reduction measures (such as resilient systems) and recovery options (including back-up facilities). In addition to traditional risks such as technical failure and disasters, new risks have emerged in recent years, such as service interruptions that are caused by security breaches—denial of service attacks, viruses, and worms.

Successful ITSCM implementation can be achieved only with visible senior management commitment and the support of all members of the organization. Ongoing maintenance of the recovery capability is essential if it is to remain effective.

The following figure shows this Business Continuity Lifecycle. Note that disaster recovery procedures are only a part of this process.

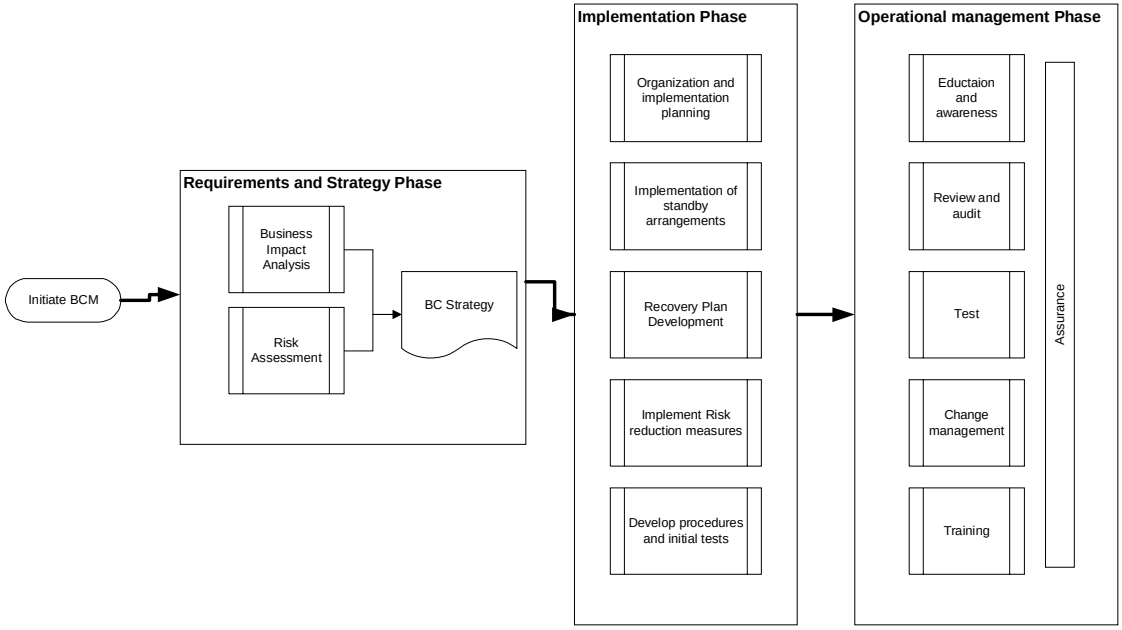

FIGURE 5-11 Business Continuity Process

Security Management

The *security management* process, as defined by ITIL, is the process of managing a defined level of security for information and IT services, including the reaction to security incidents. Security management is more comprehensive than physical security and password disciplines. It includes other core aspects, such as data integrity (financial aspects), confidentiality (intelligence agencies / defense), and availability (health care).

Security management is not an isolated process—it is an integral part of IT and the organization. The relationship between security management and other ITIL processes is such that each process has the obligation to perform the required security tasks wherever possible. These tasks in each ITIL process should address the security aspects in their specific area. However, the point of control of these tasks is centralized by the security management process.

Security management is governed by a corporate policy that drives budget, focus, and management direction. Within ITIL practices, this information is normally defined in the Service Level Agreements.

In this document, *information security incidents* are defined as events that can cause damage to confidentiality, integrity, or the availability of information or information processing. These incidents materialize as accidents or deliberate acts.

The following figure shows how security aspects and measures are applied at different stages of a potential security incident:

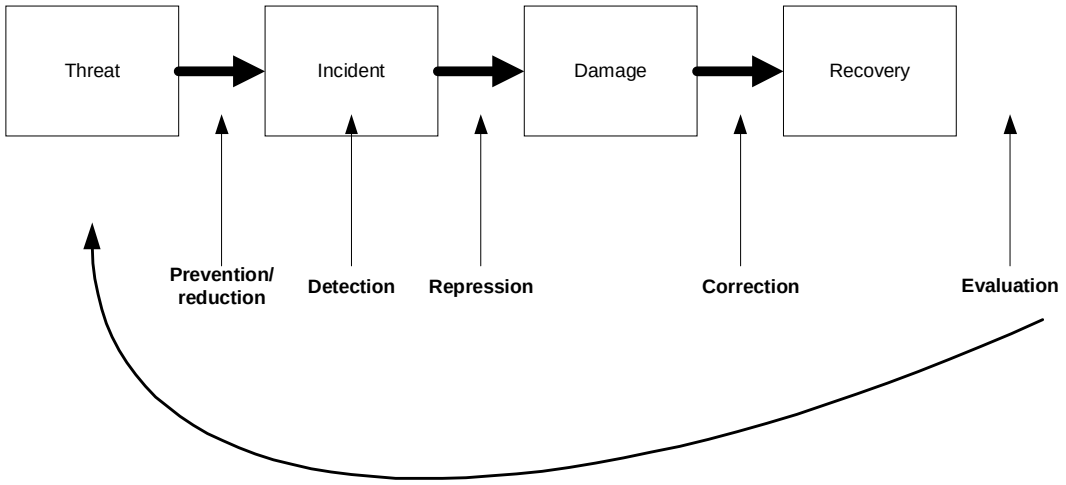

FIGURE 5-12 Security Management Process—Security Incident

The threat of a security incident to ongoing. It is the responsibility of the security management process to ensure that sufficient measures have been taken for preventing / avoiding such threats and reducing their impact. For example, disk mirroring is one approach that can prevent the loss of data resulting from an incident (failed disk), and backups that reduce the impact in case the prevention failed.

Detection is the ability to notice the fact that a security incident is in progress or has occurred. Once detected, repressive measures can then be taken to counteract the attempt, such as virus detection software with quarantine options, or account lock-outs after numerous failed login attempts.

If damage occurs the corrective procedures are activated. Like in the virus scanning software has options to repair infected files or the restore (or rebuild) of a corrupted database. A key function of security management is the evaluation and the subsequent suggestions for changes (if needed) to prevention, reductive, repressive and corrective measures.

Implementing an effective security management process should result in a business management that is realistically reassured that a sufficient level of confidentiality, integrity, and availability has been achieved.

The following figure shows how the security management process is a continuous improvement process driven by Service Level Agreements as they are defined in each ITIL process.

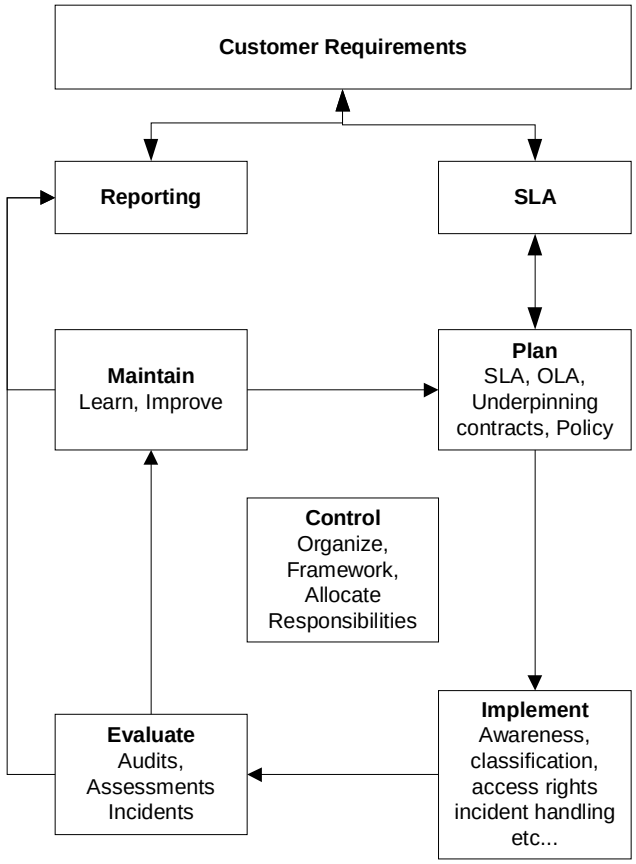

FIGURE 5-13 Security Management as a Continuous Improvement Process

6

Sun IT Management Framework—Tools

This chapter describes the *tools* aspect of the Sun IT Management Framework. It contains the following sections:

- Overview of the Sun ITMF Tools Aspect
- Tools of the Sun ITMF Tools Aspect
  - Instrumentation Types
  - Element and Resource Management Applications
  - Event and Information Management Applications
  - Service Level Management Applications
  - Workflow and Portal Systems

Overview of the Sun ITMF Tools Aspect

The *tools aspect* of the Sun ITMF describes the technology used to facilitate and automate the execution of the various IT management processes.

Manual and Automated Processes

In theory, an organization should be able to reach a high degree of operational capability by focusing on the implementation of well defined processes executed by an empowered and knowledgeable staff. Any function performed by a system's management tool could conceivably be performed by a human being instead. In this line of reasoning, the implementation of management technology is not a necessary condition for the operation of the IT environment.

However, practical considerations make this approach less than optimal and—in some cases—impossible to implement.

An Example Process—Log File Inspection

For example, a common activity in the management of systems using the Solaris™ Operating System is the periodic review of system log files for messages that indicate potential or current error conditions. Performing this task is a very basic operation that requires minimal skills. An operator with this responsibility would login to the server in question, open the appropriate system log file (such as `/var/adm/messages`), and read each entry looking for critical system messages that might require some type of action. The operator would repeat this manual inspection on every server.

Problems with the Manual Approach

This manual inspection approach, though feasible, suffers from two problems: poor scalability and human error.

Poor Scalability

The manual inspection approach is limited by some maximum number of servers per operator. The time required to complete a manual review of all servers within the operator's area of responsibility is a function of the number of servers. Even if the operator only reviews system logs, the time between successive reviews of the

same system (polling cycle) increases every time a new server is added. Because the polling cycle dictates how quickly an error is recognized, there is an upper limit to the number of servers a single operator can monitor. The only way to keep the polling cycle within acceptable parameters is a costly one—add more operators as the server count increases.

Human Error

The manual inspection approach involves human error. Humans are not capable of performing any task with a 100 percent accuracy rate all of the time, especially when repetitive and relatively mundane tasks, such as reviewing systems logs, are involved. An error condition that is caught one time by the operator might be missed any other time. Therefore, this solution cannot guarantee consistency of performance and integrity in the resulting information.

Automation Addresses These Problems

Any reasonably competent systems administrator would immediately apply technology to address these two problems. They could write a simple script that searches the log file for particular patterns (critical system messages) and generates some type of notification (page or email) whenever the pattern is found. The script could be kicked off on a periodic basis by the UNIX scheduler.

Automation addresses the scalability problem because each new server is provided a copy of the script. The operator now just deals with the exception conditions. Automation addresses the consistency issue because a well-written program performs the same with each invocation. Once a script is capable of identifying an error condition, it will always identify the condition.

Tools and Tool Categories

The discussion of manual versus automated processes leads to the definition of *tool* used in this document. Within the Sun ITMF, a *tool* is defined as any *technology that automates the execution of IT management process activities.* Automation enables IT departments to scale management of the IT environment in a reasonable, cost effective manner while ensuring that process activities are performed in a consistent fashion. In this document, related tools are grouped into general *tool categories.*

Diagram of the Sun ITMF Tools Aspect

The following figure shows the Sun ITMF tools aspect and its components:

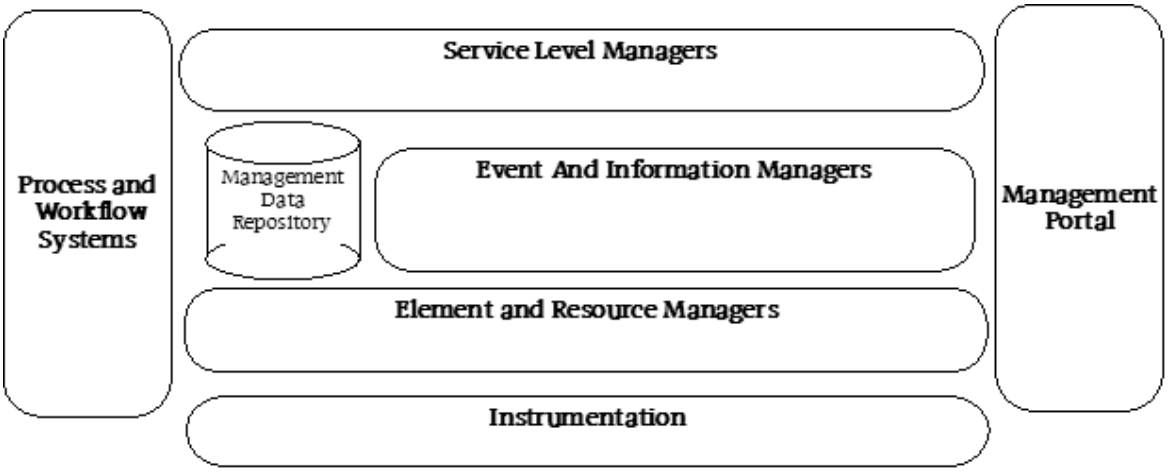

FIGURE 6-1 Sun ITMF—Tools Aspect

Tools Framework

This figure shows what we refer to in this document and within the Sun ITMF as the *tools framework*—a tiered (layered) combination of management applications integrated as appropriate to support an associated set of processes. In addition to the different layers of the framework, certain components (process and workflow systems, and management portal components) provide functionality that spans across the layers and exposes them to the external environment.

Layers of the tools framework are used to categorize management applications based on the nature of their interaction with the managed environment. Applications in the lowest levels of the tools framework interact directly with the managed environment. Applications in higher levels of the tools framework deal with more abstract issues, such as events and performance data. Applications within the portal or process workflow components expose the other elements of the framework to the IT stakeholders and process architecture, respectively. Finally, applications at the service level management layer provide the tie between the management infrastructure and the supported business processes.

Note that the categorization of tools in this fashion does not mean that a specific product cannot fill more than one role or have components that work at different levels. For example, the Sun™ Management Center product spans multiple layers, providing basic monitoring functionality for the Solaris environment (Element and

Solaris™ Resource Manager) and, with an expansion module, performing transaction testing of common network services like DNS and IMAP (Service Level Manager).

Components of the Tools Framework

The tools aspect of the Sun ITMF consists of the following components:

- Instrumentation Layer
- Element and Resource Management Layer
- Event and Information Management Layer
- Service Level Management Layer
- Process and Workflow Managers
- Management Portal
- Management Data Repository (MDR)

Instrumentation Layer

The *instrumentation layer* of the tools framework consists of all management elements that allow the various management tools to gain access to the system resources that they manage. In the context of the Execution Framework, instrumentation is generally implemented where managed resources reside. Tools in this layer are most tightly coupled with the components of the managed environment and are most directly impacted by changes to the managed environment. For example, for different operating systems (such as Solaris, Linux, and Windows), different versions of the same vendor's instrumentation are required.

Element and Resource Management Layer

The *element and resource management* layer of the tools framework consists of management applications that interact directly with the Execution Environment to query or modify managed resources. This interaction is generally conducted via the instrumentation layer. Although this layer is one step removed from the managed environment, there remains a dependency on the nature of what is being managed. For example, the application used to administer the naming service might vary depending on whether the naming service is LDAP or Microsoft Active Directory.

Event and Information Management Layer

The *event and information management* layer of the tools framework consists of applications that manage the data or events resulting from the activities of the other layers. Whereas the element and resource management layer generates *alarms* and collects *data*, the event and information management layer generates *events* and provides the mechanisms to turn data into *information*.

The definitions in the following table help clarify these kinds of distinctions.

TABLE 6-1 Definitions for the Tools Framework

Term	Definition
alarm	A notification resulting from a specific managed object state. For example, a monitor can be checking for a given situation, such as a server CPU being utilized at levels approaching 100 percent. At each sampling interval, the CPU busy metric is checked. If it is 95 percent or higher, then the application generates some type of indication (flashing icon, entry in an alarm log, etc.) that this condition exists. This indication is what we are calling an alarm.
event	A notification of an actionable condition that is inferred from one or more alarms. *Actionable* means that we need to take some action as a result of the detected condition. An event is essentially a consolidation or correlation of alarms using additional information. Using the previous example of a server CPU utilization monitor, based on knowledge of the environment, you might want to tool to flag the condition only if the CPU is 100 percent busy for three consecutive sampling intervals, at which point we should investigate the cause of the condition and take remedial action. An event is the notification resulting from three successive samplings in which the 100 percent CPU utilization alarm was triggered.
data	Consists of facts that obtained about the managed environment through management activities. For example, the CPU utilization monitor tool collects a fact (CPU busy value) every time it performs the sampling operation. The tool could store these facts and create an historical set of data points concerning the use of the CPU over a given time period.
information	Knowledge obtained by the processing and analysis of data. For example, a graph of the CPU utilization samples over time could show that the server CPU is 100 percent busy during the same time period every day. This knowledge could result in remedial action, such as moving the application to a server with faster or more CPUs.

The event and information management layer is yet another level removed from the managed environment. At this point in the model, the abstraction is sufficient to result in a very loose dependency between the applications and the managed environment. For example, the deployment of a new, different operating system should have little impact on the event management application. As long as the monitoring application for the new system produces well formed alarms, the event management application simply treats it as another source to be processed.

Service Level Management Layer

The *service level management* layer of the tools framework involves applications that provide the link between organization requirements, as defined by Service Level Agreements (SLAs), and the technical status of the execution environment, as determined by the lower layers of the framework. At the service level management layer, the focus shifts to managing the services provided by IT to support specific business processes. Service level management tools deal with the entire service chain. We define the *service chain* in this document as the combination of execution environment components, along with other services, that work together to provide a specific service.

Process and Workflow Managers

Process and workflow managers of the tools framework consist of technology that is used to automate and control the execution of the management processes described on the Sun ITMF process aspect. These include tools that facilitate the execution of specific processes, such as service desk operations or configuration management. It also includes technologies that would be used to facilitate the integration of different IT processes.

Management Portal

The *management portal* is a collection of applications that provides external entities with access to selected portions of the tools framework. Examples include a web interface for reviewing SLM reports, web or other types of user interfaces for the various tools, or an application used by end users to submit requests for service. It should also be possible—even desirable—to use this portal to expose management information and facilities to people outside of the IT organization.

Management Data Repository (MDR)

One output of management activity is data. Because significant amounts of data are generated and used in the execution of IT operations, it needs to be stored and available for use. The *management data repository* (MDR) is the *logical* representation of the entities responsible for the storage and management of IT operational data. We emphasize that this is a logical representation. In realizing the management framework, data will be stored and maintained by a number of tools at different levels of the framework. Very few, if any, working implementations have successfully deployed a single data store for all management data.

Tools Framework Touch Points

The following figure shows the interactions (touch points) between the Sun ITMF tools aspect and other entities within the IT environment.

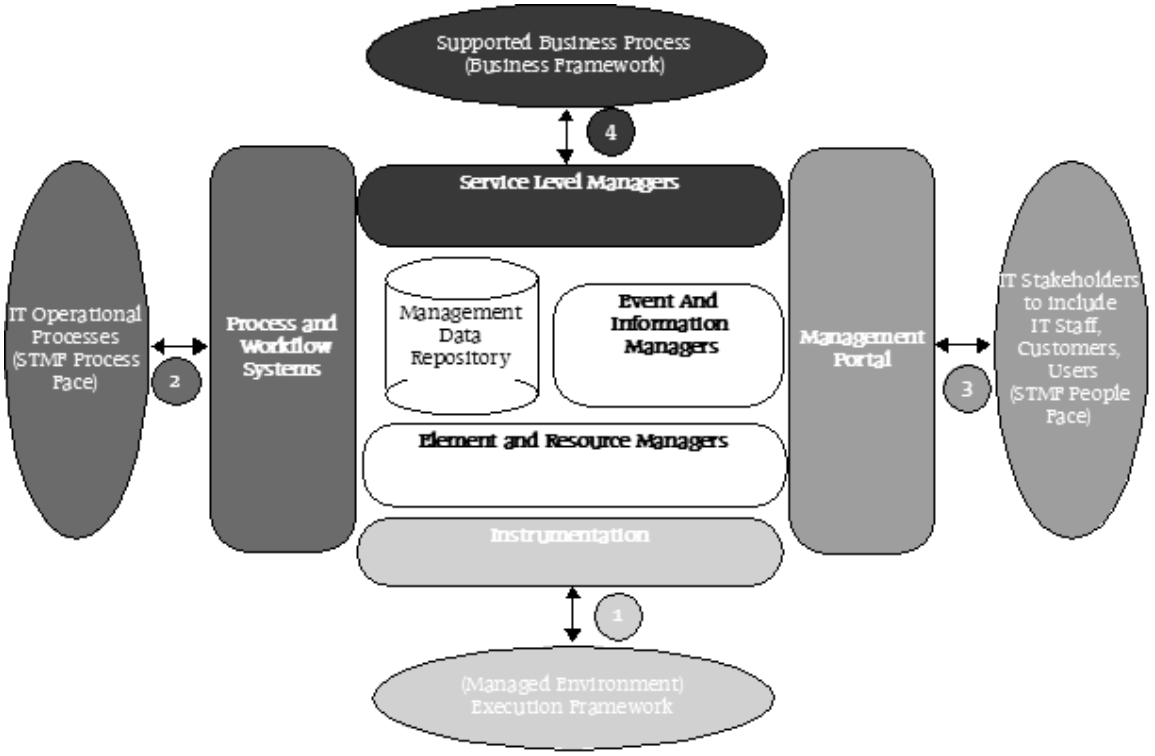

FIGURE 6-2 Sun ITMF Tools Aspect—Touch Points to the IT Environment

This figure shows how:

- The tools framework interacts with the managed environment via the instrumentation layer, which provides the hooks necessary to allow for reading and manipulating managed entities.
- The tools framework interacts with the process aspect of the Sun ITMF via the process and workflow applications.
- Management systems information and functionality is exposed to the IT stakeholders via the management portal.
- The services necessary to the execution of the organization's business are managed by the applications in the service level management layer. These applications have an understanding of the service chain that delivers a specific service, as well as an understanding of the relationships between a given service and the business processes it supports.

Tools of the Sun ITMF Tools Aspect

This section describes the tools associated with the Sun ITMF tools aspect. Tools are grouped according to the following categories:

- Instrumentation Types
- Element and Resource Management Applications
- Event and Information Management Applications
- Service Level Management Applications
- Workflow and Portal Systems

The following figure shows a detailed view of the Sun ITMF tools aspect.

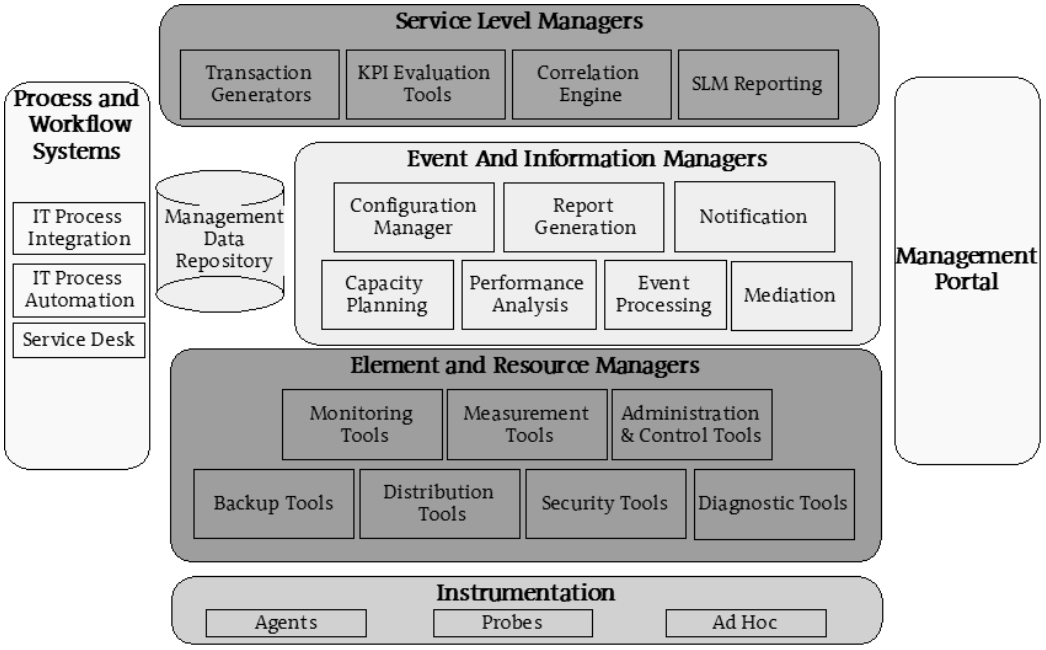

FIGURE 6-3 Detailed View of the Sun ITMF Tools Aspect

Instrumentation Types

The *instrumentation types* tool category includes:

- Agents
- Probes
- Ad Hoc Solutions

The following figure shows these tools:

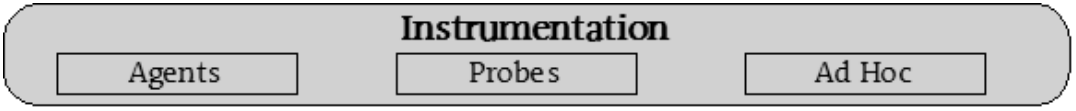

FIGURE 6-4 Tools in the Instrumentation Types Layer

Instrumentation components may or may not be provided as part of a management component in another layer. Certain management tools include agent technology as part of the product. By contrast, hardware and software vendors may provide an

agent with their product that is capable of communicating with other vendors' management tools via a defined protocol (such as the Simple Network Management Protocol, or SNMP).

Agents

Agents are software entities within the execution framework that communicate with management applications in the management framework using a defined protocol and naming scheme for managed objects. Examples include a SNMP agent that ships with a router, or a proprietary agent, such as the one that is part of the BMC PATROL solution.

Probes

Probes are special-purpose management components (hardware and software) that operate in the execution environment to perform specific management functions on behalf of management applications. Probes are stand-alone devices, while agents are generally installed on a component with another purpose. Examples include a network device that provides SNMP Remote Monitoring (RMON) functionality, or a special purpose computer that generates synthetic transactions for service level testing.

Ad Hoc Solutions

Ad hoc solutions refer to scripts and executables that operate autonomously on components within the execution framework. These components generally do not communicate with, or act on behalf of, a management application.

Element and Resource Management Applications

The *element and resource management tools* category includes:

- Monitoring Tools
- Measurement Tools
- Administration and Control Tools
- Backup Tools
- Diagnostic Tools
- Security Tools
- Distribution Tools

The following figure shows the tools that reside in the element and resource management layer.

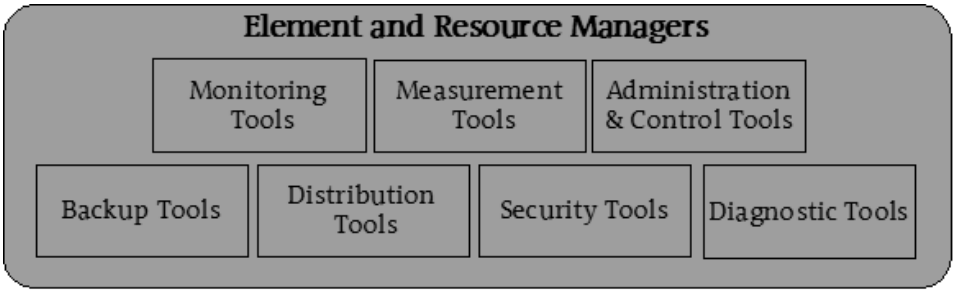

FIGURE 6-5 Tools in the Element and Resource Management Layer

Monitoring Tools

Monitoring tools sample the values of specific managed objects and compare these values to a pre-defined threshold. In most cases, threshold violations result in the generation of some type of notification (alarm). This monitoring includes both simple activities (such as testing for network connectivity or CPU utilization), as well as more complex actions (such as scanning a system log for a predefined pattern). Examples of monitoring tools include Sun Management Center for the Solaris environment, BMC PATROL for application layer entities, and Aprisma Spectrum for the IP network layer.

Measurement Tools

Because the applications that process data reside in different parts of the tools framework, it is necessary to collect this data and then make it available for use by the applications. *Measurement tools* collect data from the managed environment and then facilitate its movement to other tools within the tools framework. Measuring differs from monitoring because the results of sampling activity are maintained.

Managing and moving the sometimes large amounts of data may require the use of different instrumentation technology from what is being used to perform monitoring activities. SNMPv1 is a useful protocol for monitoring solutions. However, the nature of the protocol makes it inefficient for bulk data transfer. SNMP managed devices might require a different mechanism to move performance data.

Measurement tools are not limited to the collection of performance data. They can also capture configuration and asset information, such as hardware information, installed software, patch levels, and so on.

Examples of measurement tools include the Teamquest Performance Framework, the BGS collection agent for BMC PATROL, and the Sun Management Center Performance Reporting Manager add on.

Administration and Control Tools

Administration and Control tools are used to maintain the runtime configuration of managed resources, or to modify the execution state of a managed resource. These systems provide method access and update name service databases, user profiles, and other administrative data stores. They are also used to perform such tasks as shutdown, startup, modification of runtime priority, or restart. Examples of administration and control tools include Solaris Resource Manager, BMP PATROL for Automated Dynamic Reconfiguration, the iPlanet™ Administration Server, and the Solaris™ Management Console.

Backup Tools

Backup tools provide a mechanism to copy, archive and, if necessary, recover enterprise data. Backup systems can also manage backup media (tape management). An example of a backup system is the Sun StorEdge™ Enterprise Backup Software.

Diagnostic Tools

Diagnostic tools are applications that facilitate data collection and test execution in order to identify the root cause of an error condition. An example diagnostic system is the Sun™ Management Center Hardware Diagnostic Suite.

Security Tools

Security tools work to prevent or detect unauthorized use of IT resources, such as applications that monitor for intrusions, that access the vulnerabilities of different systems, and that perform digital forensics and data recovery activities.

We are careful to differentiate between security applications that are deployed as part of the management framework and security solutions that are deployed as part of the execution environment. Authentication and access control mechanisms, such as single sign-on applications and firewalls, are both examples of security components that are part of the execution framework.

Examples of security systems include tools such as Tripwire, COPS and Satan.

Distribution Tools

Distribution tools provide the mechanisms needed to transfer and install software, such as OS images, patches, or application software, within the execution framework. Examples of distribution tools include Sun Jumpstart™, Sun N1™ Grid, and Computer Associates' Unicenter Software Delivery.

Event and Information Management Applications

The *Event and information management* tools category includes:

- Event Processing Tools
- Performance Analysis Tools
- Capacity Planning Tools
- Mediation Tools
- Notification Tools
- Configuration Management Tools
- Report Generation Tools

The following figure shows the tools that reside at the event and information management layer of the tools framework.

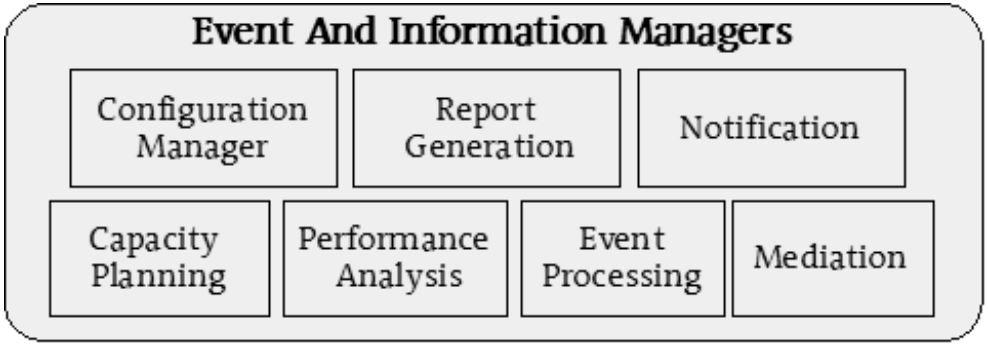

FIGURE 6-6 Tools in the Event and Information Management Layer

Event Processing Tools

Event processing tools are responsible for managing alarms generated by other layers of the framework. Specific event processing activities include:

TABLE 6-2 Event Processing Activities

Activity	Description
event filtering	Discarding of unneeded events.
event consolidation	Combination of like events.
event mapping	Transformation of event attributes to standard scheme.
event correlation	Parallel processing of events to make inferences concerning the root cause.

Examples of event processing systems include Micromuse Omnibus (Netcool) and the Tivoli Event Console (TEC).

Performance Analysis Tools

Performance analysis tools are used to visualize and analyze performance data collected by measurement applications for the purpose of identifying performance bottlenecks. Performance analysis tools are reactive rather than predictive in nature because they deal with system activity that has already occurred. Examples of performance analysis tools include Teamquest View and BMC Perform.

Capacity Planning Tools

Capacity planning tools are used to analyze performance data, along with knowledge or application workload drivers, in order to make predictions about the impact of changes on performance. Capacity planning tools differ from performance analysis tools in that they are *predictive* in nature. These tools use modeling, simulation, or other heuristics to assess the impact of expected changes to workloads and configurations so that "what if" analyses can be performed. Examples of capacity planning tools include Teamquest Model and BMC Predict.

Mediation Tools

Mediation tools bridge the gap between lower layer data collection mechanisms (measurement tools) and external systems used for charge back or billing. Mediation tools provide a means of taking performance data from a wide variety of sources and providing the preprocessing necessary to allow the application of rating and discount parameters by a billing system. Functions preformed by the mediation tools include:

- Collection of detailed performance data from lower level management tools.
- Processing of collected data to check for syntactical correctness and format as necessary.
- Summarizing the data at a level of detail necessary for the application of billing policy.
- Providing the resulting information (Call Detail Report or CDR) to the billing systems.

Notification Tools

Notification tools facilitate the process of passing information (alarms, warnings, etc.) to external entities, such as people and other applications. Notification tools are generally used to support paging and email forwarding of events to the appropriate staff. This mechanism may also be used as a means of forwarding event information to applications that are not part of the management infrastructure. Basic notification tools act as a simple gateway for events. More robust notification tools have support for managing the notification process, such as scheduling and call back verification features.

Many of these tools are developed by the IT organization. An example of a commercially available tool solution is a combination of Halcyon's PrimeAlert EventAction and InstantPaging software.

Configuration Management Tools

Configuration management tools are used to maintain information about the configuration of elements within the execution environment and their relationships to each other. This includes applications that manage:

TABLE 6-3 Components Associated with Configuration Management Tools

Component	Description
Configuration Management Database (CMDB)	Virtual database that contains asset and configuration information.
Definitive Hardware Store (DHS)	Storage for field replaceable hardware components.
Definitive Software Library (DSL)	Repository of all software master copies.

In many cases, this functionality is combined with process and workflow management tools (discussed in a subsequent section) that control the execution of such IT processes as change and configuration management. From a technical perspective, we differentiate between the maintenance of a configuration data store and the control of processes that use this information.

A simple example of a configuration management tool is a spreadsheet used to track an organization’s asset and configuration information. More complex examples includes the Remedy Asset Management for IT asset control and CVS for software configuration maintenance.

Report Generation Tools

Report generation tools are used to generate both periodic and ad hoc reports about the IT environment. These tools convey the past performance and current state of the IT environment. Reporting at this level is IT focused, in contrast to the business focused reporting seen at the next layer (service level management) of the model. A majority of the technologies used at the event and information management layer include some type of reporting mechanism. An example would be Micromuse Netcool Reporter.

Service Level Management Applications

Service level management applications provide the technical connection between the IT services (as delivered by the IT organization), and the business processes that they support. Service level management tools include:

- Transaction Generators
- KPI Evaluation Tools
- Correlation Engines
- Service Level Management Reporting
- Process and Workflow Systems
- Management Portals

The IT Service Management Forum (itSMF) defines a *service* as "an integrated composite that consists of a number of components, such as management processes, hardware, software, facilities and people, that provides a capability to satisfy a stated management need or objective."[8]

The people and process aspects of service delivery are covered on the people and process aspects, respectively, of the Sun ITMF. In the tools aspect, it is the operation of the hardware and software components that are managed at this level. The following figure shows the components at the service level management layer.

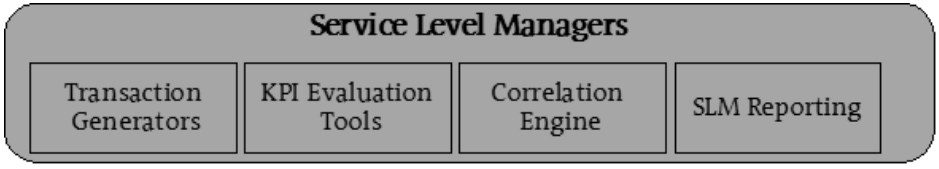

FIGURE 6-7 Tools in the Service Level Management Layer

Business and IT think differently about the technology being provided in the management of services. For example, a user might focus on the perceived responsiveness and reliability of a web application, while the IT staff might focus

8. *A Dictionary of IT Service Management Terms, Acronyms and Abbreviations*, The IT Service Management Forum, December 2001.

instead on the availability of the network, and the system and application components used to deliver it. Lewis[9] refers to this issue as the *semantic disparity problem*. Service level management is seen as the method used to bridge the gap between the business and IT. However, the challenge is being able to effectively monitor the services that are being provided within the context of an associated service level agreement.

There are two potential approaches to addressing this issue:

- **User-centric Approach**. In this approach, the performance of the service is measured in a fashion that most closely approximates the user experience.
- **Techno-centric Approach**. In this approach, low-level component parameters are considered objective measures of the higher level service's performance.

In both approaches, the goal is to evaluate the entire service chain so that the current state of the service can be inferred with a high degree of accuracy. Service level monitoring approaches that ignore critical components of the service should be avoided. Note that the two approaches are not mutually exclusive—they can be used together to provide service level monitoring. Services are deployed in support of business processes, and true service level management solutions will include a mechanism to assess business impact.

Transaction Generators

Transaction generator tools introduce workloads on a specific service and evaluate the level of response received. The workload is designed to mimic the activities of a service consumer. This testing enables the IT organization to track the service performance of both, and to evaluate the service from the perspective of the end user. These tools enable IT organizations to implement a user centric approach to service level testing and compliance monitoring. Examples of this technology includes Sun Management Center Service Availability Manager, Micromuse Internet Service Monitor, Proxima Centauri, and Mercury Interactive LoadRunner.

KPI Evaluation Tools

Key Performance Indicator (KPIs) are metrics that service as descriptive or predictive indications of a services availability and performance. *KPI evaluation tools* collect and aggregate these KPIs. Aggregation is key because a single KPI is rarely sufficient to monitor the entire service chain. KPI evaluation tools enable IT organizations to implement a techno-centric approach to service level testing. An example of a KPI evaluation tool is Proxima Centauri.

9. *Service Level Management for Enterprise Networks*, Lundy Lewis, Artech House, Boston, 1999.

Correlation Engines

Correlation engines provide the mechanism to assess the business impact of conditions (such as failures, capacity issues, alarms, or other occurrences in the managed environment) that exist within the IT environment. This level of correlation should not be confused with other impact or root cause analysis functions that may be performed by different tools within the other layers of the framework. Correlation engines have an understanding of the relationships between services and the business processes they support. Examples of correlation engines includes Micromuse Impact and the BMC Service Impact Manager.

Service Level Management Reporting

Service-level management (SLM) reporting tools facilitate real-time and historical reporting of IT's compliance with Service Level Agreements. This reporting is focused outward to the business rather than inward to the IT-centric reporting that is provided in the event and information management layer. Several of the service level management tools described earlier in this section provide the ability to generate and publish reports.

Workflow and Portal Systems

Workflow tools and *portal technology* include the following tools:

- Process and Workflow Systems
- Management Portals

These tools are used to facilitate process automation and access to management information. The following figure shows how these types of applications fit into the tools framework.

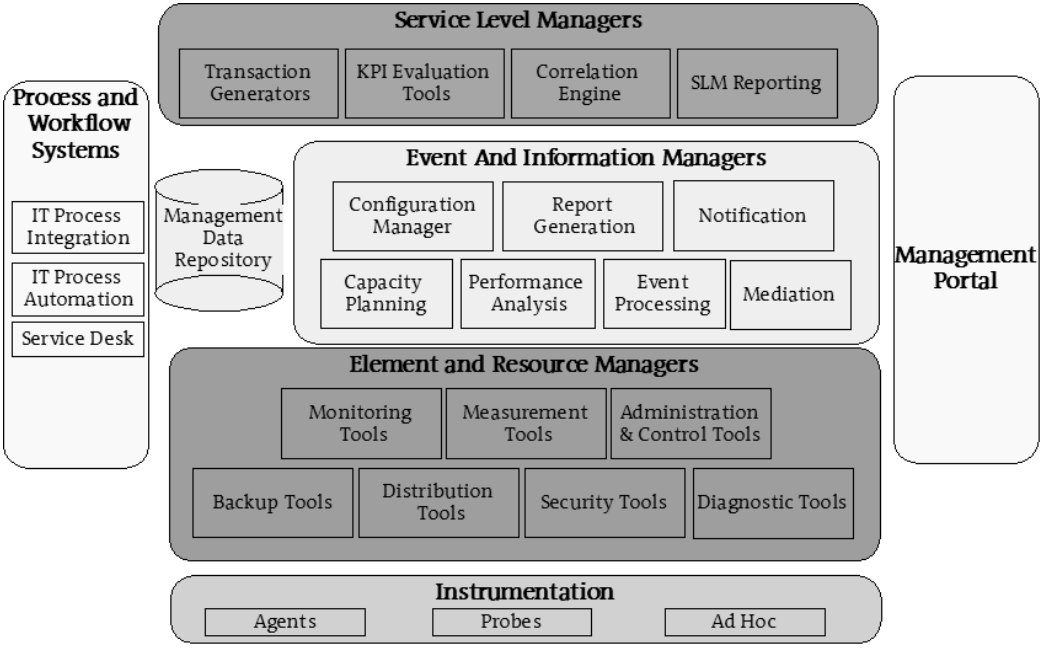

FIGURE 6-8 Tools in the Workflow and Portal Layers of the Sun ITMF

Process and Workflow Systems

Process and workflow systems are applications that can be used to automate the management processes described on the process aspect of the Sun ITMF. As shown in FIGURE 6-8, "Tools in the Workflow and Portal Layers of the Sun ITMF," on page 82, this technology may be focused on addressing three different types of automation functions:

TABLE 6-4 Automation Functions in Process and Workflow Systems

Function	Description
Service Desk	A service desk provides an organizational point of contact for requesting IT services. Service desk workflow tools automate and facilitate the interaction between IT and the external stakeholders. The service desk serves as the entry point to the IT services delivery structure.
IT Process Automation	The various management processes defined on the process aspect of the Sun ITMF are excellent candidates for automation. The IT process automation components of the Sun ITMF are tools used to control the execution of these processes. Activities include the management of request of routing, the generation of notifications, and escalation.
IT Process Integration	These provide integration between processes, as well as integration of the workflow systems and other portions of the Sun ITMF. Completion of a specific request for given service involves the execution of multiple processes and the use of various portions of the tools framework. Where the process steps supported by process automation tools are tightly joined, the interaction enabled by process integration tools is based on a loose coupling of components via some type of messaging bus. This approach allows the various processes and management components to operate in a relatively independent fashion while contributing to the completion of the service request. This loose coupling also means that processes and tools may be changed with minimal impact.

Examples of service desk and process automation technology include the Remedy Action Request System and the Network Associates Magic Help Desk. Process integration examples include the Collaxa Business Process Execution Language (BPEL) server and the Intalio N^3 Business Process Management System.

Management Portals

Management portals are collections of applications that provide external entities with access to selected portions of the management framework, such as a web interface for reviewing SLM reports, web or other types of user interfaces for the various tools, or an application used by end users to submit requests for service.

The management portal is a loosely defined concept within the Sun ITMF. In its simplest form, it could be a collection of product specific web interfaces that provide access to the various tools within the framework. In a more complex form, it could

be a true portal that provides content and application aggregation, personalization, and the facilities to control access to the management infrastructure through the implementation of user roles and entitlements.

2

Part 3—Operations Management Capabilities Model Specification

This part of the document is the specification of the Operations Management Capabilities Model (OMCM). It includes the following chapters:

- Chapter 7, “OMCM Specification—Overview”
- Chapter 8, “OMCM Specification—People”
- Chapter 9, “OMCM Specification—Process”
- Chapter 10, “OMCM Specification—Tools”

7

OMCM Specification—Overview

In Part 2, “Sun IT Management Framework,” we detailed the management framework that is used to describe the components of operational maturity. In Part 3, “Operations Management Capabilities Model Specification,” we provide the details of the OMCM itself.

This chapter provides an introduction to the components of the OMCM. It has the following sections:

- OMCM Levels and Profiles
- Structure of the OMCM

OMCM Levels and Profiles

Like most evolutionary models, the OMCM is based on the concept of different capability levels. We describe five levels of operational capability:

- OMCM Level 1—Crisis Control
- OMCM Level 2—IT Component Management
- OMCM Level 3—IT Operations Management
- OMCM Level 4—IT Service Management
- OMCM Level 5—Business Value Management

Each level is a generalization of the organization's service delivery characteristics. We believe that organizations must pass through each level. The structure of the OMCM is designed so that it is not possible to reach OMCM Level 3 without satisfying the requirements of OMCM Levels 1 and 2. This is the concept of strict ordering that is described by Niessink and Hans van Vliet. In Part 3, we detail the degree to which the Sun ITMF has been realized at each level.

OMCM Level 1—Crisis Control

At OMCM Level 1, crisis control is best characterized as immature or chaotic. At this level, there has been little effort towards creating a management infrastructure. Investment has been minimal and the organization delivers IT services via the efforts of heroes. Activities are focused on the maintenance and management of individual components within the IT infrastructure. The organization is reactive and IT users tend to find problems. OMCM Level 1 represents the starting state of our model. No focused effort is required for organizations to reach this level. We like to say that OMCM Level 1 is reached when IT shows up for work in the morning.

OMCM Level 2—IT Component Management

In OMCM Level 2, some investment in the development of the management infrastructure has been made. However, investments tend to be focused on specific problems and are not guided by an overall strategy. The tools infrastructure provides some basic visibility and protection. When needed, component information can be found and used to support the delivery of IT services. Core IT processes are beginning to be formalized in some fashion, but this effort is still in the very early stages. The level of service delivery is inconsistent due to the fact that most processes are still not defined. Most organizations reach OMCM Level 2 without structured efforts to address IT operational problems.

OMCM Level 3—IT Operations Management

At OMCM Level 2, the organization shifts from management of IT components to management of the operational aspects of IT. This is characterized by a more proactive approach to operations of the infrastructure, with technology focused on anticipating problems or reducing the impact through faster resolution. End user applications are categorized and prioritized to allow for the allocation of scarce IT resources in a more efficient manner. Service delivery becomes more formal and repeatable.

Reaching OMCM Level 3 requires that the organization have an epiphany regarding the nature of, and solutions for, its IT operational problems. The realization is that ensuring the delivery of IT services requires a holistic approach that addresses all of the components of operational capability.

OMCM Level 4—IT Service Management

At OMCM Level 4, the service delivery capabilities of the IT organization is predictable and repeatable. The IT organization manages itself by Service Level Agreements (SLAs), both internally and externally. IT processes are efficient and effective. The IT capabilities are consistent and measurable. Reaching OMCM Level 4 generally occurs when the organization shifts from being an operations organization to being a service delivery organization.

OMCM Level 5—Business Value Management

At OMCM Level 5, the IT organization is focused on process improvement and adding quantifiable value to the business. The data available from the management infrastructure is used to modify processes in order to gain efficiencies.

Traceability from the business metrics to the IT metrics allows decisions and process improvement in one area to be based on information from the other. For example, direct traceability from revenue to a service availability number could be used to evaluate IT expenditures that would increase service availability. An example of the reverse would be the analyzing of data on how customers navigate a web site to determine the effectiveness of different marketing messages.

Innovation in service delivery is now possible. For example, classes of service based on more complex pricing models may be used. OMCM Level 5 is reached through the application of continuous improvement methodologies such as Sigma.

Structure of the OMCM

The OMCM describes the realization of the Sun ITMF over time. To specify how much of the framework has been realized at each level, we use a standard format for each individual component. The OMCM describes the degree to which each process has been implemented.

- For the people aspect, the specification describes the degree to which each practice has been implemented within the organization.
- For the process aspect, the specification describes the degree to which each process has been implemented within the organization.
- For the tools aspect, the OMCM helps to assess the degree to which the tools infrastructure has been implemented, as well as the soundness of that implementation.

Degrees Of Implementation

The different levels of the OMCM are categorizations of an organization's service delivery characteristics. We use a degree of implementation description to characterize the extent to which an individual component of capability has been realized by the organization. The OMCM defines five potential degrees of implementation:

- Ad Hoc
- Emerging
- Functional
- Effective
- Optimized

The definition of each degree depends upon the component being discussed. The characteristics of a functional IT operational process will be described differently from the characteristics of a functional monitoring infrastructure. However, this scoring mechanism allows us to use consistent terminology for all three portions of the Sun ITMF, and it simplifies application of the model to real situations.

Once we describe the degree of implementation, we map the various degrees to the OMCM levels. This mapping allows us to create a capabilities profile that describes the degree of implementation for every component at a given OMCM level. This profile is then used to determine an organization's OMCM level.

We realize that this approach is more complex than some other models that simply describe each component as being at one of *x* maturity levels. We use this alternative approach because we feel that various portions of the management infrastructure develop at different times. Capturing the concept that components evolve at different points in an organization's development requires a mechanism to distinguish between individual component evolution and the capability level of the organization.

For example, the incident management and Sigma-based process improvement are implemented to different degrees at OMCM Level 3. Incident management is at a functional level, while the Sigma process is emerging. In some cases, the degree of implementation for a given component may not change from level to level.

This approach has the advantage of providing a means to prioritize investments in operational capability. For example, an OMCM Level 2 organization that is moving to OMCM Level 3 may have some components that are implemented to a sufficient degree for OMCM Level 3, while other components are not. To achieve OMCM Level 3, the focus of investment should be on those components that are not yet implemented to the appropriate degree for OMCM Level 3.

Format of the OMCM Specification

This section describes the format used to specify each element in the OMCM.

Component Heading

Name of the component.

Description

A brief *description* of the area under consideration. Most areas are described in detail in the Sun ITMF chapters of this document.

Critical to Quality

Critical to Quality defines a list of key items that should considered by organizations as they evaluate the component, such as:

- key enablers for success
- specific items that must be in place in order to properly address the component
- recommendations based on experience in implementing the component in question

This list of examples, though certainly not comprehensive, shows how the scope of these items can range from tactical to strategic.

Criteria

Criteria provides defining characteristics for each level of implementation, as shown in the following table. Criteria is used to characterize the degree of implementation for a given component.

TABLE 7-1 Criteria

Degree of Implementation	Criteria
Ad Hoc	[characteristic(s) for this level of implementation]
Emerging	[characteristic(s) for this level of implementation]

TABLE 7-1 Criteria *(Continued)*

Degree of Implementation	Criteria
Functional	[characteristic(s) for this level of implementation]
Effective	[characteristic(s) for this level of implementation]
Optimized	[characteristic(s) for this level of implementation]

Metrics

Metrics have predictive or descriptive measures that describe the component's level of implementation. These values are provided as means to help in benchmarking an organization as it works on improving operational capability. These lists of metrics are by no means exhaustive nor definitive. However, in all cases, metrics represent measurable quantities. Multiple data types are used, including:

- *numeric values* (such as the number of service requests per day)
- *Boolean values* that represent the presence or absence of a specific item or practice (such as the existence of a management architecture document for the enterprise)

Capabilities Profile

The following table details the degree of implementation required at each OMCM level.

TABLE 7-2 Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

At the end of each chapter, a summary table shows the capabilities profile for all of the components is provided.

8

OMCM Specification—People

The *people aspect* of the OMCM identifies the key people-oriented activities that are critical for an organization to understand and use to correlate their current maturity level via measurable criteria. This chapter describes the practice areas that can be assessed for maturity, as well as the criteria to use to help move the organization to the next desired OMCM level. This model can be used as the framework for developing the organization using industry accepted best practices.

This chapter provides the details for determining the degree of implementation for each of the organization or people components of the management framework. It includes the following sections:

- Organizing
- Resourcing
- Skills Development
- Workforce Management
- Knowledge Management
- Summary of the People Capabilities Profile

For an introduction to these practice areas, see Chapter 4, “Sun IT Management Framework—People.” For more information about how each practice area is described (Description, Critical to Quality, Criteria, Metrics, and Capabilities Profile), see “Format of the OMCM Specification” on page 91.

Organizing

The *organizing practice category* aligns the work being done with the goals of the organization. Any work being done that does not support the organization's goals can be identified and eliminated. The roles and responsibilities are identified to successfully achieve the goals. The overall IT organization is structured based on these roles and responsibilities. The organizational structure is defined down to the individual workgroups, and all workgroup interfaces are identified.

This practice category includes the following practices:

- Communication / Coordination
- Workgroup Development
- Workforce Planning
- Participatory Culture
- Empowered Workgroups
- Competency Integration
- Organizational Performance Alignment

Communication / Coordination

Description

Establishes a culture for openly sharing information across organizational levels and among dependent workgroups.

Critical to Quality

- Information is shared effectively across the entire organization.
- Individuals and workgroups coordinate their activities to effectively accomplish their objectives.
- Communication and coordination practices are institutionalized to ensure that they are performed as defined by organizational practices.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-1 Communication / Coordination—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Communications are unorganized and inconsistently delivered.
Emerging	• Information is shared across the organization. • Meetings are conducted to make the most effective use of each individual's time.
Functional	• The organization's workforce-related policies and practices are communicated to the workforce. • The information required for performing committed work (work that the workgroup has committed to complete) is shared across affected workgroups in a timely manner. • The interpersonal communication skills necessary to establish and maintain effective working relationships within and across workgroups are developed.
Effective	• Individuals are able to raise concerns and have them addressed by management. • Individuals' opinions on their working conditions are sought on a periodic and event-driven basis. • Individuals and workgroups monitor and coordinate the dependencies involved in their committed work.
Optimized	• Individuals and workgroups coordinate their activities to accomplish committed work.

Metrics

- Roles and team structure are defined and documented.
- Individual responsibilities are identified, as are task gaps and overlaps across workgroups within the IT organization.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-2 Communication / Coordination—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Functional	Effective	Effective	Optimized

Workgroup Development

Description

Defines common workgroup methods and procedures used to perform standard activities.

Critical to Quality

- Workgroups are established to optimize the performance of interdependent work.
- Workgroup staffing activities focus on the assignment, development, and future deployment of the workforce competencies.
- Workgroup development practices are institutionalized to ensure that they are performed as defined by organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-3 Workgroup Development—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Workgroups are not aligned with the organizational objective.
Emerging	• Workgroups are formed to perform a defined set of business activities. • Objectives are set out for the group and individuals.
Functional	• Committed work within a group is analyzed to identify its process dependencies. • The skills needed to perform assignments are identified. • Workgroup performance is managed and measured.
Effective	• Formal communications are established between groups.
Optimized	• Workgroup development practices are institutionalized to ensure that they are performed as defined by organizational processes.

Metrics

- Organizational objectives and goals are known and understood.
- Work activities are mapped to organizational objectives and goals.
- Work activities are categorized as core, support, or boundary.
- The required skills needed to perform assignments are documented.
- Role-based learning paths are defined.
- Individual and team skill gaps are identified, and training plans are in place.
- Collaboration tools and methodologies are in place and used between workgroups.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-4 Workgroup Development—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Workforce Planning

Description

Ties the organization's workforce activities directly to its business strategy and objectives.

Critical to Quality

- Measurable objectives for capability for each of the workforce competencies are defined.
- The organization plans for the workgroup competencies needed to perform their current and future business activities.
- Workforce planning practices are institutionalized to ensure that they are performed as defined by the organizational practices.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-5 Workforce Planning—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Workforce capabilities are not defined or understood.
Emerging	• Current workforce needs are documented.
Functional	• Measurable objectives are established for developing the organization's capability in each of it's workforce competencies. • The organization establishes and maintains a strategic workforce plan to guide it's workforce practices and activities. • A skills development plan is produced for each workforce competency.
Effective	• The organization plans for the workforce competencies needed to perform its current and future business activities. • The organization's performance in meeting the objectives of its strategic workforce plan is tracked.
Optimized	• The organization performs planned workforce activities to satisfy current and strategic competency needs. • Skills development plans are reviewed and revised on a periodic and event-driven basis.

Metrics

- Organizational objectives and goals are known and understood.
- Work activities are mapped to organizational objectives and goals.
- Work activities are categorized as core, support, or boundary.
- Skill profiles related to customer specific work, goals, and the IT environment are developed and in place.
- Areas where skill levels do not meet requirements and expectations—both for the individual and team—are identified.
- Training plans are in place defined education and training events are implemented.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-6 Workforce Planning—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Participatory Culture

Description

A participatory culture begins with providing individuals an understanding of the organizations goals and how their participation contributes to achieving them.

Critical to Quality

- Information about the business activities and results is communicated throughout the organization.
- Decisions are delegated to the appropriate level.
- Participatory culture practices are institutionalized to ensure that they are performed as defined by organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-7 Participatory Culture—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No formal communications processes exist. Communication is inconsistent and by word of mouth.
Emerging	• Information about organizational and workgroup performance is made available.
Functional	• Workgroups understand how their work supports the organization. • Decision-making processes and roles are defined.
Effective	• Decisions made by those empowered to make them are supported by the organization. • Individuals and workgroups use defined decision-making processes.
Optimized	• Individuals and workgroups are involved in the decision-making process.

Metrics

- Roles and team structure are defined and documented.
- Individual responsibilities, as well as task gaps and overlaps across workgroups, are identified within the IT organization.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-8 Participatory Culture—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Empowered Workgroups

Description

Empowering workgroups involves preparing individuals to work independently within the constraints of the organizational goals and objectives.

Critical to Quality

- Empowered workgroups are delegated responsibility and authority over their work processes.
- Empowered workgroups practices are institutionalized to ensure that they are performed as defined organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-9 Empowered Workgroups—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No formal processes are in place that allow for the delegation of responsibility and authority over workgroup processes.
Emerging	• The organization begins the development and performance of empowered workgroups. • Empowered workgroups are formed with a statement of their charter and authority for completion.
Functional	• Empowered workgroups are delegated the responsibility and authority to determine the methods they will use to accomplish committed work. • The organization's workforce practices are tailored for use with empowered workgroups.
Effective	• Responsibility and authority for performing selected workforce activities is delegated to empowered workgroups. • Empowered workgroups perform the workforce activities delegated to them.
Optimized	• Empowered workgroups participate in managing their performance.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- Job descriptions are in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-10 Empowered Workgroups—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Fun	Optimized

Competency Integration

Description

Creates efficiencies for each workgroup by integrating all of the processes of the individual workgroups.

Critical to Quality

- The competency-based processes of the various workgroups are integrated to improve overall organizational efficiency.
- Competency integration practices are institutionalized to ensure that they are performed as defined in the organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-11 Competency Integration—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Workgroups function separately with no integrated processes.
Emerging	• Activities involving dependencies among multiple workforce competencies are identified. • Integrated competency-based processes are defined and made available for use.
Functional	• Skills needed for performing integrated competency-based processes are developed. • The work environment supports work by individuals or workgroups using integrated competency-based processes.
Effective	• Organizational structures support multi-disciplinary work that integrates competency-based processes. • Workgroups use integrated competency-based processes for work involving multiple workforce competencies.
Optimized	• Workforce practices are designed to support multi-disciplinary work. • Workforce practices and activities are defined and adjusted to support integrated competency-based processes.

Metrics

- Skill profiles related to customer specific work, goals and IT environment are developed and in place.
- Areas where skill levels do not meet requirements and expectations both for the individual and team are identified.
- Training plans are in place defined education and training events are implemented.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-12 Competency Integration—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Organizational Performance Alignment

Description

Aligning the performance results of the individuals and workgroups with the stated objectives and goals of the organization and business objectives.

Critical to Quality

- Alignment among individuals, workgroups, and the organization is continuously improved.
- Measurable objectives are defined for the individual, workgroup, and organization.
- Organizational performance alignment practices are institutionalized to ensure that they are performed as designed by organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-13 Organizational Performance Alignment—Criteria

Degree of Implementation	Criteria
Ad Hoc	• There is no alignment between individuals, workgroups, and the organization.
Emerging	• Organizational objectives are documented and used as the basis for developing workgroups and individuals' objectives.
Functional	• The organization aligns performance across workgroups with the organizational business objectives.
Effective	• The impact of workforce practices and activities on performance alignment is managed and measured.
Optimized	• Evaluations of the impact of workforce practices and activities on performance alignment are used in performing other business and workforce activities. • The impact of workforce practices and activities on aligning individual, workgroup and organizational performance is continuously improved.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- Job descriptions, staffing level estimates, and team structure are defined and in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-14 Organizational Performance Alignment—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Ad Hoc	Emerging	Optimized

Resourcing

The *resourcing practice category* focuses on hiring or selecting the right people with the right skills to achieve an organization's goals and objectives. It also focuses on retaining top talent within the organization. Replacement costs alone can be substantial. More importantly, hiring candidates who do not possess the right skills can impede organizational progress and productivity. Selection tools and good practices are created to help managers make better decisions about who is the most qualified candidate for the job. Retention programs address the source of turnover problems and target interventions to avoid loss of critical IT personnel.

This practice category includes the following practices:

- Staffing
- Competency Analysis
- Organizational Capability Management
- Continuous Capability Improvement

Staffing

Description

Establishes a formal process in which committed work is matched to existing workgroups, and qualified individuals are recruited, hired, and placed into assignments.

Critical to Quality

- Staffing decisions and work assignments are based on an assessment of work qualifications and other valid criteria.
- Individuals transition into and out of positions in an orderly way.
- Staffing practices are institutionalized to ensure that they are performed as managed processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-15 Staffing—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No staffing processes exist.
Emerging	• Each workgroup analyzes its proposed work to determine the effort and skills required. • Recruiting is conducted for open positions. • Representative members of a workgroup participate in the hiring activities.
Functional	• Staffing decisions and work assignments are based on an assessment of work qualifications and other valid criteria. • A selection process and appropriate selection criteria are defined for each open position. • Responsible individuals plan and coordinate the staffing activities of their units in accordance with documented policies and procedures.
Effective	• Each unit documents work commitments that balance its workload with available staff and other required resources. • Individual work assignments are managed to balance committed work among individuals and workgroups.
Optimized	• Measurements are made and used to determine the status and performance of staffing activities.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- Selection tools that measure key job qualifications—performance indicators / aptitude tests, knowledge tests, and structured interview guides—are developed and administered.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-16 Staffing—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Emerging	Functional	Effective	Optimized	Optimized

Competency Analysis

Description

Identifies the workgroup competencies needed to perform the business activities that the workgroup services. Such competencies are required to fulfill the needs of the business. For example, a workgroup might need to provide tools, either through buying or developing them. Workgroup competency descriptions are periodically reviewed to ensure that they still meet the business activities.

Critical to Quality

- The workforce competencies required to perform the organization's business activities are defined and updated as necessary.
- The organization tracks its competencies in each of the workgroups.
- Competency analysis practices are institutionalized to ensure that they are performed as defined by the organizational practices.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-17 Competency Analysis—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No compilation of workforce competencies exists.
Emerging	• The workforce competencies required to accomplish business activities are identified. • Information about the use of competency-based processes is captured and made available.
Functional	• Each of the organization's workforce competencies is analyzed to identify its requisite knowledge, skills, and process abilities. • Current resource profiles for each of the organization's workforce competencies are determined.
Effective	• Current resource profiles for each of the organization's workforce competencies are determined. • Competency information regarding the capabilities of individuals in their workforce competencies is collected and maintained according to a documented procedure.
Optimized	• The organization tracks its capability in each of the workforce competencies. • Competency information is updated on a periodic and event-driven basis.

Metrics

- Work activities are mapped to organizational objectives and goals and are categorized as core, support, or boundary.
- Job responsibilities and criteria for job qualification and performance are defined.
- Skill profiles are developed and in place.
- Areas where skill levels do not meet requirements and expectations both for the individual and team are identified.
- Skills development and employee performance results are managed, tracked, measured and periodically reviewed.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-18 Competency Analysis—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Organizational Capability Management

Description

The level of skills, knowledge, and process available within the workgroups to perform the committed work. The analysis is performed at the individual level to determine the total skills, knowledge, and process abilities available within the workgroups.

Critical to Quality

- The impact of workgroup practices and activities on the capabilities of competency-based processes (in critical workgroup competencies) is evaluated and measured.
- Organizational capability management practices are institutionalized to ensure that they are performed as defined by organizational practices.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-19 Organizational Capability Management—Criteria

Degree of Implementation	Criteria
Ad Hoc	• The interrelationship of each workgroup's competencies is unknown across the entire organization.
Emerging	• The organization identifies the workforce competencies that are critical to its business strategies and objectives. • Measurable objectives for contributing to the growth in critical workforce competencies are established for workforce practices and activities.
Functional	• Process performance baselines are developed and maintained for critical competency-based processes. • The capabilities of competency-based processes in critical workforce competencies are established and managed quantitatively.
Effective	• The organization uses its capability data and process performance baselines when developing quantitative models of performance.
Optimized	• The definition and use of measures at the individual, workgroup, and unit levels are periodically audited for compliance with organizational procedures.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- Selection tools that measure key job qualifications—performance indicators / aptitude tests, knowledge tests, and structured interview guides—are developed and administered.
- Skills development and employee performance results are managed, tracked, and measured.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-20 Organizational Capability Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Continuous Capability Improvement

Description

The purpose of continuous capability improvement is to provide a foundation for individuals and workgroups to continuously improve their capability for performing competency based processes.

Critical to Qualify

- The organization establishes and maintains mechanisms for supporting continuous improvement of its competency-based processes.
- The capabilities of competency-based processes are continuously improved.
- Continuous capability improvement practices are institutionalized to ensure that they are performed as defined by organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-21 Continuous Capability Improvement—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Competency-based processes are not documented or understood.
Emerging	• Individuals characterize the capability and performance of their personal work processes. • Individuals evaluate the capability of their personal work processes to identify opportunities for improvement.
Functional	• Workgroups evaluate the capability and performance of their operating processes to identify opportunities for improvement. • Workgroups establish measurable objectives and plans for improving the capability of operating processes. • Workgroups continuously improve their capability and performance.
Effective	• The capabilities of competency-based processes are continuously improved. • Within each critical workforce competency, capability objectives are defined for critical competency-based processes. • Within selected workforce competencies, responsible individuals identify, evaluate, and select improvements to competency-based processes.
Optimized	• Measurements are made to determine the effectiveness of continuous capability improvement.

Metrics

- Skills development and employee performance results (paper or system) are managed, tracked, measured, and periodically reviewed.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-22 Continuous Capability Improvement—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Ad Hoc	Functional	Optimized

Skills Development

The *skills development practice category* includes:

- performing skills analysis at the individual and team levels
- identifying skill gaps based upon the defined role(s) for which the individual and team is responsible
- providing learning events (such as training, mentoring, and coaching) to fill identified skill gaps
- certifying skills and knowledge

Using the results from the skills analysis, skill development plans and learning paths are developed for the individual and the team to help them gain the skills necessary to perform their roles. The learning path allows the individual to obtain the skills necessary for projected future roles. Skills analyses are repeated periodically to help ensure that the required skills have been obtained.

This practice category includes the following practices:

- Training and Development
- Career Development
- Competency Development
- Mentoring

Training and Development

Description

The purpose of training and development is to close the gaps between an individual's current skills and those necessary to perform their assignments. Training plans are developed that prioritize the critical skills needed to perform the assignment. The results of the training plan are tracked in the workgroup's training plan.

Critical to Quality

- Individuals receive timely training that is needed to perform their assignments in accordance with the workgroup's training plan.
- Individuals capable of performing their assignments pursue development opportunities that support their development objectives.
- Training and development practices are institutionalized and performed as a managed process.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-23 Training and Development—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Training is done on a case by case basis with no formal training or development plan.
Emerging	• In each workgroup, the critical skills required for performing each individuals assigned tasks are identified. • Training needed in critical skills is identified for each individual.
Functional	• Each workgroup develops and maintains a plan for satisfying its training needs. • Training is tracked against the unit's training plan.
Effective	• A development discussion is held periodically with each individual.
Optimized	• Individuals capable of performing their assessments pursue development opportunities that support their career development objectives.

Metrics

- Customer-specific skill profiles are developed.
- Existing skill levels are analyzed.
- Individual and team development plans are created.
- Targeted training is implemented.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-24 Training and Development—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Functional	Effective	Optimized	Optimized

Career Development

Description

Career development is used to enable the individual to see the organization as a vehicle for achieving their career goals. It ensures that the individual develops workforce competencies that will allow them to achieve their career goals.

Critical to Quality

- The organization provides career opportunities to encourage growth in their workgroup competencies.
- Individuals pursue career opportunities that increase the value of their knowledge, skills, and process abilities to the organization.
- Career development practices are institutionalized to ensure that they are performed as a managed process.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-25 Career Development—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No formal training plans exist.
Emerging	• The organization defines graduated career opportunities to support the growth of the workforce competencies required to perform its business activities.
Functional	• Career promotions are made in each area of graduated career opportunities based on documented criteria and procedures.
Effective	• Graduated career opportunities and promotion criteria are periodically reviewed and updated. • Affected individuals keep a personal development plan to guide their training and career options. • Career options and development in the organization's workforce competencies are discussed with individuals on a periodic or event-driven basis.
Optimized	• Individuals pursue career opportunities that increase the value of their knowledge, skills, and process abilities to the organization.

Metrics

- Succession plan is in place.
- Customer-specific skill profiles are developed.
- Existing skill levels are analyzed.
- Individual development plans are created.
- Targeted training is implemented.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-26 Career Development—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Competency Development

Description

The purpose of competency development is for the organization to constantly enhance the ability of the workgroups to deliver on the assigned business objectives.

Critical to Quality

- Individuals develop their knowledge, skills, and process abilities in the workgroup competencies.
- Workgroups uses their workgroup skills to develop the skills of others in the workgroup.
- Skills development practices are institutionalized to ensure that they are performed as defined by the organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-27 Competency Development—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Skills are not understood or documented at the individual or workgroup level.
Emerging	• The organization provides opportunities for individuals to develop their capabilities in its workforce competencies.
Functional	• Role-based training and development activities are identified for each individual to support their development objectives. • Graduated training and development activities are established and maintained for developing capability in each of the organization's workforce competencies.
Effective	• Individuals develop their knowledge, skills, and process abilities in the organization's workforce competencies.
Optimized	• The organization uses the capabilities of its workforce as resources for developing the workforce competencies of others.

Metrics

- Customer-specific skill profiles are developed.
- Existing skill levels are analyzed.
- Individual and team development plans are created.
- Targeted training is implemented.
- Internally-driven mentoring and coaching program are established.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-28 Competency Development—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Mentoring

Description

Mentoring transfers the knowledge and expertise of more experienced individuals or individuals with scarce skills to other members of the workgroup.

Critical to Quality

- Mentoring programs are established and maintained to accomplish defined objectives.
- Mentors provide training and/or guidance to individuals and workgroups.
- Mentoring practices are institutionalized to ensure that they are delivered according to organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-29 Mentoring—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Mentoring is informal and happens in an inconsistent manner.
Emerging	• Mentors assist individuals or workgroups in developing capability in workforce competencies. • Opportunities for using the experience of the workforce to improve performance or achieve other organizational objectives are identified.
Functional	• Mentoring programs are established and maintained to accomplish defined objectives. • Mentors and those they mentor establish a mentoring relationship. • Mentors are selected and matched with individuals or workgroups to be mentored.
Effective	• Each mentoring program is communicated to affected individuals and workgroups. • Mentors support the development and improvement of competency-based assets.
Optimized	• Mentoring relationships are reviewed to ensure that they satisfy their intended results.

Metrics

- Mentoring and coaching activities / programs are defined and implemented.
- On-going support programs are established.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-30 Mentoring—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Workforce Management

The *workforce management practice category* involves managing the day to day administration of employees, including compensation, work environment, communication, training plans, providing feedback through performance reviews, and other activities targeting employee needs.

This practice category includes the following practices:

- Work Environment
- Staff Performance Management
- Compensation
- Quantitative Performance Management

Work Environment

Description

The purpose is to establish and maintain the physical working environment and to provide the resources needed for individuals to perform their tasks effectively and without unnecessary distractions.

Critical to Quality

- The work environment is provided to allow individuals to accomplish their tasks.
- The environment is set up to minimize distractions.
- Work environment practices are institutionalized to ensure that they are performed as managed services.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-31 Work Environment—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No processes exist for managing the work environment.
Emerging	• The physical environment and resources required to perform committed work are identified for each workgroup. • The physical environment required to perform assigned work is provided.
Functional	• Individual workspaces provide an adequate personal environment for performing assigned work responsibilities. • The resources needed to accomplish committed work are provided in a timely manner.
Effective	• Improvements are made to the work environment to improve work performance. • Physical factors that degrade the effectiveness of the work environment are identified and addressed.
Optimized	• Distractions in the work environment are minimized.

Metrics

- Work space and ergonomic assessments are completed with corrective actions.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-32 Work Environment—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Functional	Effective	Optimized	Optimized

Staff Performance Management

Description

Objectives are established at the individual level and are based on the workgroup's objectives needed to achieve their committed work. Periodic reviews are conducted with the individual to assess achievement and continuing relevance of the objectives.

Critical to Quality

- Workgroup and individuals objectives are documented to ensure that business objectives are accomplished.
- Periodic reviews of objectives are conducted.
- Performance problems are managed.
- Reward and recognition occurs.
- Staff performance management practices are institutionalized to ensure that they are performed as managed services.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-33 Staff Performance Management—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No formal processes exist for managing performance. • Feedback is provided verbally.
Emerging	• Measurable performance objectives based on committed work are established and documented for each unit.
Functional	• Performance objectives for each individual are documented and reviewed on a periodic or event-driven basis.
Effective	• Guidelines for recognizing and rewarding outstanding performance are developed and communicated. • Performance problems are managed. • Potential improvements in process, tools, or resources—that could enhance an individual's performance of committed work—are identified, and actions are taken to provide them. • The accomplishments of individuals against their performance objectives are documented and discussed on a periodic or event-driven basis according to a documented process.
Optimized	• Performance Management activities, status, and results are reviewed and updated as appropriate.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined and documented.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- A performance management program is in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-34 Staff Performance Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Functional	Effective	Optimized	Optimized

Compensation

Description

The purpose of compensation is to provide individuals with remuneration and benefits commensurate with their contribution and value to the organization.

Critical to Quality

- Compensation strategies and activities are defined, executed, and communicated.
- Compensation is equitable relative to the skills, knowledge, and contribution to the organization.
- Compensation practices are institutionalized to ensure that they are performed as managed services.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-35 Compensation—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No documented process exists for managing compensation.
Emerging	• An organizational compensation strategy is developed.
Functional	• A documented compensation plan is prepared periodically for the administering compensation activities needed to execute the compensation strategy. • The compensation plan is designed to maintain equity in administering the compensation strategy.
Effective	• Compensation is equitable relative to skill, qualifications, and performance. • Compensation adjustments are made based, in part, on each individual's documented accomplishments against their performance objectives. • Action is taken to correct inequities in compensation or other deviations from the organization's policy, strategy, and plan.
Optimized	• Compensation packages are periodically reviewed and corrected as necessary.

Metrics

- A compensation program, which includes base salary, variable pay, equity offerings and benefits, is in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-36 Compensation—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Functional	Effective	Optimized	Optimized

Quantitative Performance Management

Description

A quantitative performance management strategy is developed to identify, measure, and analyze the competency-based processes that contribute to the achievement of workgroup objectives.

Critical to Quality

- Measurable performance objectives are established for the competency-based processes that most effectively contribute to achieving workgroup objectives.
- Metrics exist to manage competency-based processes.
- Quantitative performance management practices are institutionalized to ensure that they are performed as defined by organization processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-37 Quantitative Performance Management—Criteria

Degree of Implementation	Criteria
Ad Hoc	• No measures exist for competency-based processes.
Emerging	• The quantitative performance objects required to achieve organizational business objectives are defined. • Each workgroup establishes measurable performance objectives whose achievement most contributes to organizational business objectives.
Functional	• Measurable performance objectives are established for the competency-based processes that most contribute to achieving performance objectives.
Effective	• Individuals and workgroups plan their committed work using process performance baselines for competency-based processes. • Individuals and workgroups quantitatively manage the performance of the competency-based processes that most contribute to achieving their performance objectives.
Optimized	• Quantitative records of individual and workgroup performance are maintained. • Quantitative performance results are used in performing workforce practices and activities.

Metrics

- Job responsibilities and criteria for job qualification and performance are defined and documented.
- Job requirements and expectations for job performance are documented and are aligned with the organization's objectives.
- Performance management program is in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-38 Quantitative Performance Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Functional	Effective	Optimized

Knowledge Management

The *knowledge management practice category* allows the organization to track its skills and manage its intellectual capital. Knowledge management includes the skills required, skills assessments, training plans, and any curriculum that has been developed or purchased by the organization. Continuous review occurs to identify any new skills or changes to existing skills that are necessary to ensure the competency of the organization and staff.

This practice category includes the following practices:

- Competency-Based Practices
- Competency-Based Assets
- Continuous Workforce Innovation

Competency-Based Practices

Description

The purpose of competency-based practices is to ensure that all practices are based on developing the competencies of the workgroups.

Critical to Quality

- Workgroup practices are focused on increasing the organization's capability in its workgroup competencies.
- Compensation strategies and reward and recognition practices are designed to encourage the development and application of the organization's workgroup competencies.
- Competency-based practices are institutionalized to ensure that they are performed according to organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-39 Competency-Based Practices—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Skills, knowledge, and processes are not documented or tracked. • Roles and competencies are not defined for the workgroups.
Emerging	• Workforce practices are focused on increasing the organization's capability in its workforce competency. • The workforce skills required to perform committed work are identified and documented. • Recruiting activities are planned and executed to satisfy the organization's requirements for workforce competencies.
Functional	• Each workgroup documents its performance objectives for developing workforce competencies. • Work assignments are designed, in part, to enhance personal and career development objectives. • Each individual's performance is assessed against the objectives of their personal development plan.
Effective	• Compensation practices are defined to support capability objectives within each workforce competency. • Ongoing discussions of work performance include feedback on an individual's development and application of relevant workforce competencies. • Selection processes are enhanced to evaluate each candidate's potential for contributing to organization and unit objectives for capability in workforce competencies.
Optimized	• As the definition or requirements of its workforce competencies change, the organization re-evaluates its workforce policies and practices and adjusts them as appropriate.

Metrics

- A performance management program is in place.
- Processes/tools are in place to assist managers and individual contributors in documenting the outcomes of performance mapping, development planning discussions, and skills development activities.
- Selection tools that measure key job qualifications—performance indicators/aptitude tests, knowledge tests, and structured interview guides—are developed and administered.
- A compensation program, which includes base salary, variable pay, equity offerings, and benefits, is in place.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-40 Competency-Based Practices—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Competency-Based Assets

Description

Competency-based assets captures the knowledge, experience, and artifacts developed in performing competency-based processes within an organization.

Critical to Quality

- The knowledge, experience, and artifacts resulting from performing competency-based processes are developed into competency-based assets.
- Competency-based assets are deployed and used.
- Competency-based assets are institutionalized to ensure that they are performed as defined by organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-41 Competency-Based Assets—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Skills, knowledge, experience are not formally tracked.
Emerging	• A strategy for developing and deploying competency based assets is created for each affected workforce competency. • Individuals and workgroups begin to track and retain information about competency-based processes. • Communication vehicles are established to support the sharing of competency-based assets amongst the competency communities.
Functional	• The knowledge, experience, and artifacts resulting from performing competency-based processes are developed into competency based assets. • Competency-based assets are integrated into competency-based processes and related technologies.
Effective	• Individuals and workgroups use competency-based assets in performing their business activities. • Information about competency-base assets is captured and made available across the organization. • Competency development activities incorporate competency-based assets.
Optimized	• Mentoring or coaching activities are organized to deploy competency-based assets. • Workforce practices and activities encourage and support the development and use of competency-based assets.

Metrics

- A standard documentation set has been defined.
- Documents are accessible via a repository, such as a web site, a collaboration tool or a content management system.
- A documentation set is managed, reviewed, and updated periodically.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-42 Competency-Based Assets—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Continuous Workforce Innovation

Description

Continuos workforce innovation involves establishing of processes for proposing improvement in workgroup activities, identifying needs for new practices and technologies, and implementing the most beneficial ones across the organization.

Critical to Quality

- The organization establishes and maintains mechanisms for continuous improvement of its workgroup practices and technologies.
- Innovative or improved workgroup practices and technologies are identified and evaluated.
- Innovative or improved workgroup practices and technologies are deployed in an orderly manner.
- Continuous workforce innovation practices are institutionalized to ensure that they are performed as defined organizational processes.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 8-43 Continuous Workforce Innovation—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Processes and technologies are not documented and no continuous process takes place.
Emerging	• The organization establishes a framework for continuously improving its workforce practices and activities.
Functional	• Individuals and workgroups are empowered to continuously improve their performance of workgroup activities. • Quantitative objectives are established for improving the impact of workforce practices and activities.
Effective	• A continuous improvement program is established to encourage individuals and workgroups to propose improvements to workforce practices and activities. • Data regarding the impact of the organization's workforce practices and activities are analyzed to identify areas that would most benefit from innovative or improved practices. • Innovative and improved workforce practices and technologies are evaluated and selected for implementation. • The deployment of innovative or improved workforce practices or technologies is planned and prepared.
Optimized	• The status and results of the organization's continuous workforce innovation activities are periodically reviewed and communicated across the organization.

Metrics

- A process improvement plan is defined and in place.
- A community of practice is established for the purpose of exchanging, creating, and extending best practices and tools.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 8-44 Continuous Workforce Innovation—Criteria

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Emerging	Optimized

Summary of the People Capabilities Profile

The following table summarizes the degree of implementation profile for each OMCM level of the OMCM people aspect.

TABLE 8-45 Capabilities Profile Summary of the OMCM People Aspect

Activity Area and Practice	Level 1 Crises Control	Level 2 IT Component Management	Level 3 IT Operations Management	Level 4 IT Service Management	Level 5 Business Value Management
Organizing - Communication / Coordination	Ad Hoc	Functional	Effective	Effective	Optimized
Organizing - Workgroup Development	Ad Hoc	Emerging	Functional	Effective	Optimized
Organizing Workforce Planning	Ad Hoc	Emerging	Functional	Effective	Optimized
Organizing Participatory Culture	Ad Hoc	Emerging	Functional	Effective	Optimized
Organizing Empowered Workgroups	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Organizing Competency integration	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Organizing Organizational Performance Alignment	Ad Hoc	Ad Hoc	Ad Hoc	Emerging	Optimized
Resourcing Staffing	Emerging	Functional	Effective	Optimized	Optimized
Resourcing Competency Analysis	Ad Hoc	Emerging	Functional	Effective	Optimized

TABLE 8-45 Capabilities Profile Summary of the OMCM People Aspect *(Continued)*

Resourcing Organizational Capability Management	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Resourcing Continuous Capability Improvement	Ad Hoc	Ad Hoc	Ad Hoc	Functional	Optimized
Skills Development Training and Development	Ad Hoc	Functional	Effective	Optimized	Optimized
Skills Development Career Development	Ad Hoc	Emerging	Functional	Effective	Optimized
Skills Development Competency Development	Ad Hoc	Emerging	Functional	Effective	Optimized
Skills Development - Mentoring	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Workforce Management Work Environment	Ad Hoc	Functional	Effective	Optimized	Optimized
Workforce Management Staff Performance Management	Ad Hoc	Functional	Effective	Optimized	Optimized
Workforce Management - Compensation	Ad Hoc	Functional	Effective	Optimized	Optimized
Workforce Management Quantitative Performance Management	Ad Hoc	Ad Hoc	Functional	Effective	Optimized
Knowledge Management Competency Based Practices	Ad Hoc	Emerging	Functional	Effective	Optimized
Knowledge Management Competency Based Assets	Ad Hoc	Emerging	Functional	Effective	Optimized
Knowledge Management Continuous Workforce Innovation	Ad Hoc	Ad Hoc	Ad Hoc	Emerging	Optimized

9

OMCM Specification—Process

The *process aspect* of the OMCM represents the actual IT management processes that are needed to support the IT service life cycle. The process aspect describes processes for creating, deploying, and managing IT services. This chapter explains how to determine a certain level of OMCM operation capability for the process aspect.

This chapter provides the details for determining the degree of implementation for each of the process components of the management framework. It includes the following sections:

- Overview
- Create IT Services
- Implement IT Services
- Deliver IT Services
- Improve IT Services
- Control
- Protect IT Services

For an introduction to these process components, see Chapter 5, “Sun IT Management Framework —Process.” For more information about how each process component is described (Description, Critical to Quality, Criteria, Metrics, and Capabilities Profile), see “Format of the OMCM Specification” on page 91.

Overview

This section provides an overview of process criteria and defines key terms.

Process Maturity Criteria

Unlike the tools and people aspects of the OMCM, the criteria used to determine the degree of implementation for a process are very similar across processes. Therefore, the following table describes these criteria and, to be consistent with the format for this document, each section will refer back to this table.

The following criteria have been defined for process maturity:

TABLE 9-1 Process Maturity Criteria for LOI Determination

	Process Definitions	Roles and Responsibilities	Documentation	Automation	Integration with other processes
(1) Ad-Hoc	Basically non-existent. Only the obvious steps are known.	Defined at a very high level. The boundaries are unclear. No interaction between roles, and lots of overlap and potential conflict.	**Guidelines:** Virtually non-existent and, if they exist, only verbally known. **Policies:** Non-existent **Procedures:** Non-existent	Non-existent or very sporadic and not very effective.	Non-existent
(2) Emerging	Some exist but may be incomplete. They are probably not very effective and not well communicated into the IT organization.	These are now somewhat defined but with overlaps and gaps. Although a responsibility has been assigned, the associated authority might not exist.	**Guidelines:** Some have been developed, but they are not well communicated. **Policies:** Are being developed, but are incomplete and not well communicated. **Procedures:** Some ad-hoc procedures exist, but are likely incomplete and not tested.	Some aspects are being supported by tools, but there is no comprehensive strategy.	Not well defined, but some may exist by coincidence due to personal efforts.

TABLE 9-1 Process Maturity Criteria for LOI Determination *(Continued)*

	Process Definitions	Roles and Responsibilities	Documentation	Automation	Integration with other processes
(3) Functional	Definitions are complete but not 100% effective. They have been communicated and are understood by the IT organization.	These are now well defined, with little overlap and no major gaps. The roles are also reflected in the organization, but authority is still informal or self-assigned.	**Guidelines:** Well defined, published, and communicated. **Policies:** Defined, published, and communicated. **Procedures:** Not all are completely defined. Not necessarily up to date and not completely tested.	Tools are effectively leveraged and they improve process quality.	External links have been identified. Proper handoff procedures exist. The processes are loosely coupled with external systems.
(4) Effective	Definitions are complete and propagated into the organization. They are well understood by all involved.	Well defined, with no overlap or gaps. They match the organization and some areas have also formal authority to complete their responsibilities.	**Guidelines:** Well defined, published, and communicated. **Policies:** Defined, published, and communicated. **Procedures:** All required exist and they are well maintained and tested.	Tools are effectively leveraged and they improve process quality.	External links have been identified. Proper handoff procedures exist. The processes are loosely coupled with external systems.
(5) Optimized	Definitions are complete and propagated into the organization. They are well understood by all involved.	Well defined, with no overlap or gaps. They match the organization and ***all*** areas have also formal authority to complete their responsibilities.	**Guidelines:** Well defined, published, and communicated. **Policies:** Defined, published, and communicated. **Procedures:** All required exist and they are well maintained and tested.	Tools are effectively leveraged and they improve process quality and efficiency.	External links are well defined. Proper handoff procedures exist and are efficient. The processes are now tightly coupled with external systems.

Definitions

The following definitions are used to describe the documentation aspects of the process maturity criteria:

TABLE 9-2 Definitions for Documentation Aspects of the OMCM

Term	Definition
guideline	A statement or other indication of policy or procedure by which to determine a course of action. Example: Guidelines for the completion of tax returns.
policy	A plan or course of action, as of an organization, intended to influence and determine decisions, actions, and other matters. Example: A company's personnel policy.
procedure	A manner of proceeding; a way of performing or effecting something: standard procedure. Example: A set of established forms or methods for conducting the affairs of an organized body, such as a business, club, or government.

Note that the degree of specificity increases as you move from guideline to policy to procedure.

Create IT Services

The *create IT services* process category describes all processes related to the creation of new services, including identifying, quantifying, architecting, and designing IT services. It involves:

- Determining what services are needed and desired for the IT customers.
- Defining of the relationship between IT customers and the IT service provider, including the definition of Service Level Agreements (SLAs).
- Addressing the processes that ensure the completeness of the IT service portfolio and the alignment of the IT Services with each other.
- All activities necessary to identify, quantify, architect, and design IT services.

To determine the level of capability, the key question is: Does IT deliver services according to the SLAs, and do these SLAs reflect the business requirements?

This process category includes the following process areas, which are assessed to determine the level of operational capability:

- Service Level Management

- Availability Management

Service Level Management

Description

The *service level management* process involves:

- planning, coordinating, drafting, agreeing, monitoring, and reporting on SLAs
- the on-going review of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved.

SLAs provide the basis for managing the relationship between the provider and the IT customer. An SLA is a written agreement between the IT service provider and the IT service customer(s). It defines the key service targets and responsibilities of both parties.

The existence of SLAs is a sign of higher levels of OMCM. One cannot successfully implement this process unless certain leading processes (such as problem and change management) and skills and tools are in place.

Critical to Quality

Consider the following factors when determining the level of implementation:

- Is service level management (SLM) well defined?
- How well is the service level management process implemented?
- Are operational level agreements in place with other internal suppliers (support groups)?
- Are underpinning contracts (UC) in place with external suppliers?
- Is service level reporting in place?
- Are tools in place to support SLM?
- Is a service catalogue utilized?
- Are there effective relationships with other IT service management disciplines?
- Are service management review meetings held?
- Do you have a service improvement process?
- Are SLM KPIs/quality measures used?
- Are service level management responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the SLM process:

- What number or percentage of services are covered by SLAs?
- Are underpinning contracts and OLAs in place for all SLAs and for what percentage?
- Are SLAs being monitored and are regular reports being produced?
- Are review meetings being held on time and correctly minuted?
- Is there documentary evidence that issues raised at reviews are being followed up and resolved (for example, via an SIP)?
- Are SLAs, OLAs, and underpinning contracts current, and what percentage are in need of review and update?
- What number or percentage of service targets are being met, and what is the number and severity of service breaches?
- Are service breaches being followed up effectively?
- Are service level achievements improving?
- Are customer perception statistics improving?
- Are IT costs decreasing for services with stable (acceptable but not improving) service level achievements?

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-3 Service Level Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Availability Management

Description

Availability management is the process that manages key components of the predictability and availability of IT services, assuring the ability of an IT service or component to perform its required function at a stated instant or over a stated period of time.

Availability requirements heavily influence service architecture design. Availability (or rather, unavailability) is the key indicator of service quality perceived by the organization and user. Availability is underpinned by the reliability and maintainability of the IT infrastructure and the effectiveness of the IT support organization. An IT service with a high degree of implementation has low frequency of failure and rapid resumption of service after an incident has occurred.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is availability management defined?
- How well is the availability management process defined and executed?
- How well is the cost of availability understood?
- To what level is availability planning undertaken?
- How well is the availability improvement process defined?
- To what level is measurement and reporting implemented?
- How well are methods and techniques employed within the availability management process?
- To what levels are tools used to support availability management?
- How effective are relationships with other IT service management disciplines?
- To what extend are availability management KPIs/quality measures used?
- Are the availability manager's responsibilities well defined?

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the availability process:

- Continual improvement of availability targets.
- The frequency and duration of IT service failures is reduced over time.
- The levels of additional IT availability provided are cost justified.
- The availability plan is issued as planned and reviewed within agreed timescales.
- Availability reporting reflects the business, user, and IT support organization perspectives.
- The agreed number of TOPS is executed and minuted.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-4 Availability Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Implement IT Services

The *implement IT services* process category encompasses efforts to properly roll-out of a new or updated IT service that has been created. This process category includes the following process area used to assess the level of operational capability: Release Management.

Release Management

Description

The *release management* process involves a collection of authorized changes to an IT service. A release typically consists of a number of problem fixes and enhancements to the service, the new or changed software required, and any new or changed hardware needed to implement the approved changes.

Release management is concerned with changes to defined IT services. The release management process facilitates the following activities involved in the implementation of IT services:

- Planning and overseeing the successful rollout of software and related hardware.
- Designing and implementing efficient procedures for the distribution and installation of changes to IT systems.
- Ensuring that the hardware and software being changed is traceable, secure, and that only correct, authorized, and tested versions are installed
- Communicating with, and managing the expectations of, the customer during the planning and rollout of new releases.
- Achieving agreement about the exact content and rollout plan for the release through liaison with change management.
- Implementing new software releases or hardware into the operational environment using the controlling processes of configuration management and change management. A release should be under change management and may consist of any combination of hardware, software, firmware, and documentation configuration items.
- Ensuring that master copies of all software are secured in the definitive software library (DSL) and that the Configuration Management Data base (CMDB) is updated.
- Ensuring that all hardware being rolled out or changed is secure and traceable, using the services of configuration management.

The focus of release management is the protection of the live environment, or IT service delivery environment, and its services through the use of formal procedures and checks.

Release management works closely with the change management and configuration management processes to ensure that the shared CMDB is kept up-to-date following changes implemented by new releases, and that the content of those releases is stored in the DSL. Hardware specifications, assembly instructions, and network configurations are also stored in the DSL/CMDB.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is release management defined?
- How well is the release policy defined?
- How well is the DSL defined?
- Is release planning well structured?
- How well are releases designed, built and configured?
- Is the acceptance process well defined?
- How well is release rollout planning undertaken?

- How well is release communication, preparation and training developed?
- How well is distribution and installation performed?
- To what degree are tools used to support release management?
- How effective are relationships with other IT service management Disciplines?
- Are release management KPIs / quality measures used?
- Are release management Responsibilities well defined?

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the release management process:

- Releases are built and implemented on schedule and within budgeted resources.
- Very low (preferably no) incidence of releases needing to be backed out due to unacceptable errors.
- Low incidence of build failures.
- Secure and accurate management of the DSL with no evidence of software that has not passed quality checks.
- Compliance with all legal restrictions relating to bought-in software.
- Accurate distribution of releases to all remote sites.
- The on time implementation of releases at all sites.
- No evidence of unauthorized reversion to previous versions at any site.
- No evidence of use of unauthorized software at any site.
- No evidence of payment of licence fees or wasted maintenance effort.
- No evidence of wasteful duplication in release building.
- Accurate and timely recording of all build, distribution, and implementation activities within the CMDB.
- The planned composition of releases matches the actual composition.
- The number of problems in the live environment that can be attributed to new releases.
- The number of major and minor releases per reporting period.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-5 Release Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized

Deliver IT Services

The *deliver IT services* process category is the most visible part of the IT organization's activities. This category addresses all activities that assure the proper delivery and ongoing operation of the IT services, including efforts to assure predictable, consistent service delivery. This is often referred to as *IT operations* or *data center operations*.

This process category includes the following process areas, which are assessed to determine the level of operational capability:

- Capacity Management
- Incident Management
- Capabilities Profile
- Service Desk

Capacity Management

Description

The capacity management process is responsible for ensuring that the capacity of the IT infrastructure matches the evolving demands of the organization in the most cost-effective and timely manner. The process encompasses:

- The monitoring of performance and throughput of IT services and the supporting infrastructure components
- Undertaking tuning activities to make the most efficient use of existing resources
- Understanding the demands currently being made for IT resources and producing forecasts for future requirements
- Influencing the demand for resources, perhaps in conjunction with financial management.

- The production of a capacity plan that enables the IT service provider to deliver services of the quality defined in the SLAs.

Capacity management is essentially a balancing act—balancing cost against capacity to ensure that:

- purchased processing capacity is cost justifiable in terms of the organization's needs
- priority is given to making the most efficient use of resources
- supply meets demand—the available supply of processing power matches the demands made on it by the business, both now and in the future; it may also be necessary to manage or influence the demand for a particular resource.

Critical to Quality

Consider the following factors when determining the level of implementation:

- Is capacity management well defined?
- Is the "resource capacity management" sub-process well defined?
- Is the "service capacity management" sub-process well defined?
- Is the "business capacity management" sub-process well defined?
- How well is capacity data managed?
- How well is demand management defined?
- How well are modelling activities undertaken?
- How well is the capacity plan defined?
- Is capacity management reporting implemented well?
- To what degree are tools used to support capacity management?
- Are there effective relationships with other IT service management disciplines?
- Are capacity management KPIs/quality measures used?
- Are capacity management responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the capacity management process:

- Timely production of forecasts of resource requirements.
- Accurately forecast trends in utilization.
- Incorporation of business plans into the capacity plan.
- Ability to monitor the performance of all services.
- Implementation of new technology in line with business requirements.
- Reduction in panic buying due to the implementation of the capacity planning process.
- Demonstration of no significant over-capacity.
- Accurate forecasts of planned expenditure.
- Reduction in the number of incidents due to poor performance.
- Reduction in lost business due to inadequate capacity.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-6 Deliver IT Services—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Emerging	Functional	Effective	Optimized

Incident Management

Description

The incident management process addresses the activities associated with service disruption events. The primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. A normal service operation is defined as service operation within the SLA limits.

The incident management process is closely related to the problem management process that looks to find the root cause for multiple similar incidents and has a clear goal of improving service reliability as well as other SLAs.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is incident management defined?
- How well is incident detection and recording managed?
- How well is incident classification and initial support managed?
- How well is incident investigation and diagnosis managed?
- How well are incidents resolved and recovered?
- How well is incident closure defined?
- Is the ownership, monitoring, tracking, and communication of incidents well defined?
- How well are major incidents managed?
- To what degree are tools used to support incident management?
- How effective are relationships with other IT service management disciplines?
- To what extent are incident management KPIs/quality measures used?
- Are the incident manager's responsibilities well defined?
- Is there documentation to be reviewed?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Measurable targets for objective metrics should be set for the effectiveness of the incident management process. Consider including the following KPIs and metrics:

- Total number of incidents.
- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code.
- Percentage of incidents handled within the agreed response time (incident response-time targets may be specified in SLAs, for example, by impact code).
- Average cost per incident.
- Percentage of incidents closed by the service desk without reference to other levels of support.
- Incidents processed per service desk workstation.
- Number and percentage of incidents resolved remotely, without the need for a visit.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-7 Incident Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Emerging	Functional	Optimized	Optimized

Service Desk

Description

The *service desk* process involves a central point of contact for handling customer, user, and related issues to meet customer and business objectives. This function is known under several possible names (or their variants), including:

- service desk
- help desk
- call centre
- customer hot line

The service desk extends the range of services and offers a more global-focused approach, allowing business processes to be integrated into the service management infrastructure. It handles incidents, problems, and questions. The service desk also provides an interface for other activities, such as customer change requests, maintenance contracts, software licenses, service level management, and configuration management, availability management, financial management for IT services, and IT service continuity management.

The service desk is customer-facing and its main objectives are to drive and improve service to—and on behalf of—the organization. At an operational level, its objective is to provide a single point of contact that dispenses advice, guidance, and the rapid restoration of normal services to its customers and users.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is the service desk implemented?
- How well is technology employed?
- How well are service desk responsibilities defined?
- How well is the escalation process defined?
- How well are service desk staffing requirements detailed?
- How well are customer satisfaction surveys utilized?
- How adequate is the service desk environment?
- How adequate are the service desk supporting processes and materials?
- To what extent are service desk staff trained in interpersonal skills?
- How well are the service desk processes and procedures defined?
- How well are incident metrics and reporting defined?
- To what degree are tools used to support the service desk?
- How effective are relationships with other IT service management disciplines?
- To what extent are service desk KPIs/quality measures used?
- Are the service desk manager's responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Measurable targets for objective metrics should be set to measure service desk effectiveness. Consider the following KPIs and metrics:

- Percentage of incidents closed by first level support, second level support, and so on.
- Telephony based KPIs (for example, average wait time, maximum wait time, average call duration, or call abandon rate).
- Number of management reports delivered on time.
- Number of customer satisfaction surveys completed on time.
- All customer complaints followed up and actioned.
- Accurate and timely breakdown and workload analyses produced of incident lifecycle, by support group, third party, and so on.
- Quantity of customer training needs identified.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-8 Service Desk—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Functional	Effective	Optimized

Improve IT Services

The *improve IT services* process category addresses all activities surrounding the measurement and optimization of IT service activities with the goal of continuously improving service levels.

ITIL has included many of these components in each process, but problem management is the focal point for root cause analysis and the prevention of issues. Sun has developed Sun^{SM} Sigma to formalize a methodology to facilitate process improvement—in general and specifically in the IT environment. In combination, they create a solid foundation to facilitate continuous service level improvement.

This process category includes the following process areas, which are assessed to determine the level of operational capability:

- Problem Management
- Continuous Process Improvement

Problem Management

Description

The *problem management* process involves:

- minimizing the adverse impact of incidents and problems on the organization that are caused by errors within the IT infrastructure
- preventing the recurrence of incidents related to these errors

In order to achieve this goal, problem management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation.

The problem management process has both reactive and proactive aspects.

- *Reactive problem management* is concerned with solving problems in response to one or more incidents.
- *Proactive problem management* is concerned with identifying and solving problems and Known errors before incidents occur in the first place.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is problem management defined?
- Are problem control activities well defined?
- Are error control activities well defined?
- How well is proactive problem management executed?
- Are problem metrics defined well?
- To what degree are tools used to support problem management?
- How effective are relationships with other IT service management disciplines?
- To what extent are problem management KPIs/quality measures used?
- Are the problem manager's responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Measurable targets for objective metrics should be set to measure the effectiveness of the problem management process. Consider including the following KPIs and metrics:

- The number of requests for change (RFCs) raised and the impact of those RFCs on the availability and reliability of the services covered.
- The amount of time worked on investigations and diagnoses per organizational unit or supplier, split by problem types.

- The number and impact of incidents occurring before the root problem is closed or a known error is confirmed.
- The ratio of immediate (reactive) support effort to planned support effort in problem management.
- The plans for resolution of open problems with regard to resources—people, costs, and other associated resources.
- Short descriptions of actions to be undertaken.
- The expected resolution time for outstanding problems.
- The elapsed time to date on outstanding problems.
- The total elapsed time on closed problems.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-9 Problem Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized

Continuous Process Improvement

Description

Although ITIL understands the need for *continuous process improvement*, it has not defined a separate discipline to address this important aspect. The Sun ITMF uses the processes as defined by Sun internally. However, any Sun Sigma-based approach should provide sufficient rigor and commitment to sufficiently address this area.

Sun Sigma is the core methodology that Sun is using to achieve industry-leading availability and quality. Sun Sigma drives key processes with data about critical customer requirements. *Sigma* is the term used in statistical analysis for variation from perfection. Sun attains a common measurement of quality for any type of process by using data to define and control process, and then measuring defects across a project (or across the organization).

Sun Sigma refers to a methodology commonly known as Six Sigma (see http://www.isixsigma.com/). The objective of Sun Sigma is to completely satisfy customer requirements profitably. We call it Sun Sigma because not all customers will require

all of the processes to yield products or services at 6 sigma (such as 3.4 defects per million opportunities, or *DPMO*). The real challenge is to more thoroughly understand customer requirements and plan the sigma levels of the products, services, and processes accordingly.

Critical to Quality

Consider the following factors when determining the level of implementation:

- Is the Sigma process well defined?
- Are there standard Six-Sigma processes defined?
- Is continuous process improvement embedded in daily operations?
- Is there high level management support for Sigma initiatives?
- Are the progress reports published regularly?
- Are there effective relationships with other IT service management disciplines?
- Are Sigma process leader's responsibilities well defined?

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Below are some examples of KPIs that can be used to measure the level of implementation of the Sun Sigma processes.

- Duration of process improvement projects.
- ROSS (return on Sun Sigma) numbers.
- Abandoned processes.
- Customer feedback on perceived improvements.
- Have the objectives of the project been achieved?
- In a timely manner?
- Stakeholder involvement.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-10 Continuous Process Improvement—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized

Control

The *control* process category involves ensuring that IT services are delivered within the constraints identified by the governing body and includes the processes that facilitate the governing activities. Examples of governing functions are: financial controls, audit, alignment with business objectives, and so on.

This process category includes the following process areas, which are assessed to determine the level of operational capability:

- IT Service Continuity Management
- Security Management
- Change Management

IT Financial Management

Description

The *IT financial management* process involves controlling the monetary aspects of the organization. It supports the organization in planning and executing its business objectives and requires consistent application throughout the organization to achieve maximum efficiency and minimum conflict.

Within an IT organization, IT financial management it is visible in three main processes:

TABLE 9-11 IT Financial Management Processes

Process	Description
budgeting	Process of predicting and controlling the spending of money within the organization. Consists of periodic negotiation cycles to set budgets (usually annual) and the day-to-day monitoring of current budgets
IT accounting	Set of processes that enable the IT organization to account fully for the way its money is spent (particularly the ability to identify costs by customer, by service, am by activity). It usually involves ledgers and should be overseen by trained accountants.
charging	Set of processes required to bill customers for the services that the organization supplies to them. This requires sound IT accounting to a level of detail determined by the requirements of the analysis, billing, and reporting processes.

Critical to Quality

Consider the following factors when determining the level of implementation:

- Is “financial management for IT services” well defined?
- How well is budgeting implemented?
- How well is the IT accounting system developed?
- How well is the IT charging system developed?
- How well is the ongoing operation of financial management for IT services managed?
- Are tools in place to support IT financial management?
- How effective are relationships with other IT service management disciplines?
- Are financial management for IT services KPIs/quality measures used?
- Are IT financial management responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the financial management for IT services process:

- Cost recovery profiles and expenditure profiles prove to be accurate.
- Charges, where applied, are seen to be fair.
- The IT organization is provided with the expected income/level of profits.
- IT customers' and users' behavior and perceptions change.
- Plans and budgets are produced on time.
- Specified reports are produced at the required time.
- The inventory schedules are kept up-to-date.
- All costs are accounted for.
- Timeliness of annual audits.
- Meeting of monthly, quarterly, and annual business objectives.
- The number (and severity) of changes required to the IT accounting system.
- Accuracy of monthly, quarterly, and annual profiles.
- Number of changes made to the charging algorithm (where appropriate).

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-12 IT Financial Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Emerging	Functional	Optimized	Optimized

Configuration Management

Description

The *configuration management* process provides a logical model of the infrastructure or a service by identifying, controlling, maintaining, and verifying the versions of configuration items (CIs) in the organization.

The goals of configuration management are to:

- Account for all IT assets and configurations within the organization and its services.

- Provide accurate information on configurations and their documentation to support all the other service management processes.
- Provide a sound basis for incident management, problem management, change management, and release management.
- Verify the configuration records against the infrastructure and correct any exceptions.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is configuration management defined?
- How well is the configuration management plan defined?
- How well are configuration items (CIs) identified?
- How well are configuration items (CIs) controlled?
- Is configuration status accounting well defined?
- How well is configuration verification and audit undertaken?
- How well is the configuration management database (CMDB) defined and utilized?
- To what degree are tools used to support configuration management?
- How effective are relationships with other IT service management disciplines?
- To what extent are availability management KPIs/quality measures used?
- Are the configuration manager's responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Measurable targets for objective metrics should be set for the effectiveness of the configuration management process. Consider using the following KPIs and metrics:

- Occasions when the configuration is not as authorized.
- Incidents and problems that can be traced back to wrongly made changes.
- RFCs that were not completed successfully due to poor impact assessment, incorrect data in the CMDB, or poor version control.
- The cycle time to approve and implement changes.
- Licences that have been wasted or not put into use at a particular location.

- Exceptions reported during configuration audits.
- Unauthorized IT components detected in use.
- The number of changes to the CMDB per month due to identified errors in the CMDB.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-13 Configuration Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Emerging	Effective	Optimized

Change Management

Description

The *change management* process involves ensuring that standardized methods and procedures are used for efficient and prompt handling of all changes, with the goal of minimizing the impact of change-related incidents upon service quality and, consequently, to improve the day-to-day service delivery of the IT organization.

Making an appropriate response to a change request entails a considered approach to risk assessment and business continuity, change impact, resource requirements, and change approval. This considered approach is essential to maintain a proper balance between the *need* for change and the *impact* of the change.

Note that change management processes need to have high visibility and open channels of communication in order to promote smooth transitions while changes are occurring.

The basic thrust of change management is mainly process-related and managerial, rather than technical. In contrast, incident management is primarily technical, with a strong emphasis on the mechanical nature of some of the processes.

Change management is responsible for managing its interfaces with other business and IT functions. The following figure shows a sample process model of change management. This is just one example—the way in which an organization decides to implement the change management process is, to a large extent, driven by the available resources (time, priorities, people, and budget).

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is change management defined?
- How well are requests for change (RFCs) utilized?
- How well is the concept of a Change Advisory Board (CAB) applied?
- Is a Forward Schedule of Changes (FSC) well implemented?
- How well defined is the outsourced change management process?
- How well are changes categorized and prioritized?
- How well is impact and resource assessment conducted?
- How well are changes built, tested, and implemented?
- Are urgent changes clearly defined?
- How well are change reviews undertaken?
- Are change metrics defined well?
- To what degree are tools used to support change management?
- How effective are relationships with other IT service management disciplines?
- To what extent are change management KPIs/quality measures used?
- Are the change manager's responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Consider using the following KPIs and metrics to judge the effectiveness and efficiency of the change management process:

- A reduction of adverse impacts on service quality resulting from poor change management.
- A reduction in the number of incidents traced back to changes implemented.
- A decrease in the number of changes backed out.

- A low number of urgent (and therefore unplanned) changes. This should include emergency, out-of-hours changes referred back for clarification.
- No evidence of changes having been made without reference to the change management and configuration management system(s).
- Close correlation between FSCs and the actual implementation of changes.
- No high-priority RFCs in backlogs, and the size of backlogs not increasing.
- Evidence of accurate resource estimating, when resource estimates are retrospectively compared with actual resources used.
- Regular reviewing of RFCs and implemented changes, and the clearing of any review backlogs.
- Successful implementation of changes that clearly benefit the business and satisfy customers.
- A low incidence of unjustifiably rejected RFCs.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-14 Change Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Emerging	Functional	Effective	Optimized

Protect IT Services

The *protect IT Services* process category involves ensuring that IT services are still available under extraordinary conditions, such as catastrophic failures, security breaches, unexpected heavy loads, and so on. This area has become increasingly important as as organizations depend more and more on IT services. Therefore, implementing IT service protection at the right levels is crucial to an organization's strength and survival.

This process category includes the following process areas, which are assessed to determine the level of operational capability:

- IT Service Continuity Management
- Security Management

IT Service Continuity Management

Description

The *IT service continuity management* (*ITSCM*) process supports the overall business continuity management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support, and service desk) can be recovered within required and agreed upon business time constraints.

IT service continuity has become critical to an organizational survival as organizations have become increasingly dependent upon technology. Technology is a core component of most business processes.

Continuity is bolstered by implementing risk reduction measures (such as resilient systems) and recovery options (including back-up facilities). In addition to traditional risks such as technical failure and disasters, new risks have emerged in recent years, such as service interruptions that are caused by security breaches—denial of service attacks, viruses, and worms.

Successful ITSCM implementation can be achieved only with visible senior management commitment and the support of all members of the organization. Ongoing maintenance of the recovery capability is essential if it is to remain effective.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is the business continuity management strategy defined?
- How well has the ITSCM scope been defined?
- How well has the BCM plan been defined?
- How well have the requirements analysis and strategy been defined?
- How well has the BCM plan been implemented?
- How well is ITSCM process managed operationally?
- How well is the invocation process and guidance defined?
- Is there a clear management structure for BCM?
- How well is the IT service continuity management recovery plan defined?
- How effective are relationships with other IT service management disciplines?
- Are ITSCM KPIs/quality measures used?
- Are the ITSCM manager's responsibilities well defined?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

The following KPIs and metrics can be used to judge the effectiveness and efficiency of the ITSCM process:

- Are scheduled tests executed on time?
- Are audits and reviews carried out regularly?
- Are the results of the test schedule published?
- Is time taken to recover services within plan?
- How many people are passing through education and awareness programs?
- Are review meetings being held on time and accurately minuted?

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-15 IT Service Continuity Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized

Security Management

Description

The *security management* process, as defined by ITIL, is the process of managing a defined level of security for information and IT services, including the reaction to security incidents. Security management is more comprehensive than physical security and password disciplines. It includes other core aspects, such as data integrity (financial aspects), confidentiality (intelligence agencies / defense), and availability (health care).

Security management is not an isolated process—it is an integral part of IT and business. The relationship between security management and other ITIL processes is such that each process has the obligation to perform the required security tasks wherever possible. These tasks in each ITIL process should address the security aspects in their specific area. However, the point of control of these tasks is centralized by the security management process.

Security management is governed by a corporate policy that drives budget, focus, and management direction. Within ITIL practices, this information is normally defined in the Service Level Agreements.

In this document, *information security incidents* are defined as events that can cause damage to confidentiality, integrity, or the availability of information or information processing. These incidents materialize as accidents or deliberate acts.

Critical to Quality

Consider the following factors when determining the level of implementation:

- How well is the security management strategy defined?
- How well has the security management scope been defined?
- How well has the security management plan been defined?
- How well do the SLAs include security management requirements?
- How well has the security management plan been implemented?
- How well is security management process managed?
- How well are the responsibilities of the security management defined?
- Is there a centralized role for security management?
- How well are prevention, reduction, detection repression, correction, and evaluation measures implemented?
- How effective are relationships with other IT service management disciplines?
- Are security management KPIs/quality measures used?

These questions are part of Sun's more comprehensive ITIL assessment, and therefore Sun methodologies and tools are available to support answering of these questions. To remain focused on the purpose of this document, some of the ITIL assessment details have been omitted.

Criteria

For details, see TABLE 9-1, "Process Maturity Criteria for LOI Determination," on page 138.

Metrics

Below are some examples of KIP's that can be used to measure the level of implementation of the security management process:

- Number of security related incidents
- Number of security breaches
- Number of viruses / spam / worms, etc., not intercepted?
- Number of security updates to infrastructure / network / operating system / applications?
- Access accounts found for employees who have already left the organization.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 9-16 Security Management—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad-Hoc	Emerging	Functional	Optimized	Optimized

Summary of the Process Capabilities Profile

The following table summarizes the degree of implementation profile for each OMCM level for the OMCM process aspect.

TABLE 9-17 Process Capabilities Profile Summary of the OMCM Process Aspect

		Level of Implementation				
Process Category	**Process**	**OMCM Level 1**	**OMCM Level 2**	**OMCM Level 3**	**OMCM Level 4**	**OMCM Level 5**
Create IT Service	Service Level Management	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Create IT Service	Availability Management	Ad Hoc	Emerging	Functional	Effective	Optimized
Implement IT Service	Release Management	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Deliver IT Service	Capacity Management	Ad-Hoc	Emerging	Functional	Effective	Optimized
Deliver IT Service	Incident Management	Ad-Hoc	Emerging	Functional	Optimized	Optimized
Deliver IT Service	Service Desk	Ad-Hoc	Ad-Hoc	Functional	Effective	Optimized
Improve IT Service	Problem Management	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Improve IT Service	Sun Sigma	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Control	IT Financial Management	Ad-Hoc	Emerging	Functional	Optimized	Optimized
Control	Configuration Management	Ad-Hoc	Ad-Hoc	Emerging	Effective	Optimized
Control	Change Management	Ad-Hoc	Emerging	Functional	Effective	Optimized
Protect	IT Service Continuity	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Protect	Security Management	Ad-Hoc	Emerging	Functional	Optimized	Optimized

10

OMCM Specification—Tools

The *tools aspect* of the OMCM addresses the technology used to facilitate the management of the execution environment, including:

- technologies to interact with, and control, the execution environment
- technologies to control and monitor the processes used to manage the environment
- technologies that provide access to the information and capabilities of the management infrastructure for a diverse set of stakeholders

This chapter describes how to determine the degree of implementation for each of the tools components of the OMCM. It includes the following sections:

- Specification of Management Tools Architecture
- Implementation of Functional Components
- Degree of Visibility
- Integration of Components
- Process Automation
- Effectiveness of the Implementation
- Summary of the Tools Capabilities Profile

For an introduction to these tools components, see Chapter 6, “Sun IT Management Framework—Tools.” For more information about how each tools component is described (Description, Critical to Quality, Criteria, Metrics, and Capabilities Profile), see “Format of the OMCM Specification” on page 91.

Specification of Management Tools Architecture

Description

The management tools infrastructure is an IT system that is little different from other IT applications. As organizations first start to deploy management tools, their efforts tend to be stove piped and tightly focused. The design concepts are simple and generally communicated to a small group of stakeholders. The need for a formal, blueprint for construction is minimal. As the tools infrastructure matures, the implementations become more complex, involving multiple organizations and products that must function in a cooperative fashion. This drives the need for a plan that captures and documents these complexities and communicates them to a larger audience for acceptance and use. This plan is what we call the management tools architecture.

Critical to Quality

- The management tools architecture should exhibit the characteristics of any properly developed technical architecture, involving the separation of functions, well defined interfaces, and formal documentation.
- The architecture will evolve over time. A process should be in place to periodically refresh to architecture to account for changes in technology, requirements, or the organization.
- The architecture should be specified in a product neutral fashion. The addition or removal of a specific vendor's technology should not invalidate the basic architecture.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 10-1 Architecture Specification—Criteria

Degree of Implementation	Criteria
Ad Hoc	• The organization does not have any concept of a enterprise wide management architecture.
Emerging	• A tools-based architecture is focused on the deployment of individual silos.
Functional	• A tools-based architecture specifies the components and integration of the complete management architecture. • Architecture is serves as a guideline, and deviations exist.
Effective	• Management architecture provides a basis for organization standards. • Tools acquisition and deployment is controlled by the management architecture. • Deviations from the architecture are minimal and closely managed.
Optimized	• Holistic management architecture includes people and process considerations in place. • Traceability between the three components of the management architecture.

Metrics

- Existence of an architecture document or document set.
- Elapsed time because the architecture and associated documentation was reviewed and updated.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-2 Architecture Specification Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Optimized	Optimized

Implementation of Functional Components

Description

In Chapter 6, “Sun IT Management Framework—Tools,” we introduced a generalized framework for enterprise management technology. This tools framework provides a product-neutral approach for categorizing the various roles to be played by each component of the overall management tools architecture. Specific commercial or locally developed products may be used to fill one or more of the functional categorizes, depending on the needs of the organization.

Although it is conceivable, it is highly unlikely that a suppler could provide a single product that fills all of the roles described. The product based framework approach to enterprise management tools has proven to be too difficult and expensive for most organizations to deploy. As a result, the industry has moved towards the deployment of management solutions in a modular fashion. Each tool has a limited scope of functionality, which results in a faster deployment and return on investment.

In keeping with the idea that management capability develops over time, we realize that the individual functional components are deployed at different times in the organization's evolution. Part of this is driven by the nature of the various components and their interaction. For example, implementing an event management console generally requires the existence of lower level monitoring components to generate enough events to make the effort worthwhile.

The maturing of IT operational processes also results in the deployment of corresponding components of the tools model. The introduction of Service Level Agreements (SLAs) and the need to monitor performance against them results in the use of transaction generators and SLA reporting mechanisms.

Finally, the implementation of each individual functional component is a process that occurs over time. Initial deployments can be very basic, with subsequent implementations providing additional uses, customization, and complexity.

The phrase *implementation of functional components* that is used in this document refers to the number of functional components of the tools model that are deployed, as well as the degree to which each tool is implemented.

Critical to Quality.

- Tools that have been implemented for a particular function are actively used by the organization.
- Tools that have been deployed for a particular function must be actively maintained by the organization. Responsibility for this maintenance is assigned to a specific group or individual.

Criteria

Use the following criteria to determine the degree of implementation for each of the components of the management tools model. Metrics and capabilities profiles for each layer are provided in the following sections. When appropriate, additional criteria for specific areas are provided.

TABLE 10-3 Functional Components of the Tools Infrastructure—Criteria

Degree of Implementation	Criteria
Ad Hoc	• The subsystem has not been deployed.
Emerging	• The subsystem has been installed. • The subsystem is operational, although it might not always be available. • The subsystem is considered a production tool. • The subsystem has a limited role or is used occasionally by the organization.
Functional	• The subsystem is actively maintained by the organization. • The subsystem is generally available. • The organization has completed basic customization and is not completely relying on the default configuration. • The scope of the sub system's deployment is consistent with its role, and the owning organization's span of control. • The subsystem performs in a reliable manner.
Effective	• The organization has extended the customization to support specific IT process activities or organization specific requirements. • The subsystem is considered critical to IT operations.
Optimized	• The subsystem is deployed in a highly available configuration.

Element and Resource Managers

Element and resource managers consist of management applications that interact directly with the execution environment to query or modify managed resources.

TABLE 10-4 Element and Resource Managers

Application	Description
Monitor	Applications that sample the values of specific managed objects and compare these values to a pre-defined threshold. In most cases, threshold violations result in the generation of some type of notification (alarm).
Measure	Applications that sample values associated with specific managed objects and store these values for subsequent review and analysis by other applications within the framework.
Administer and Control	Applications used to maintain the runtime configuration of managed resources, or to modify the execution state of a managed resource. These systems provide method access and update name service databases, user profiles, and other administrative data stores. They are also used to perform such tasks as shutdown, startup, modification of runtime priority, or restart. Administration applications are used to maintain the runtime configuration of managed resources. Examples include applications used to change host resolution tables, user identification and entitlement databases, or runtime parameters for an application.
Backup	Applications that collect images of a specific managed resource (data) for use in data recovery efforts if data is compromised due to a system failure or user error.
Diagnose	Applications that facilitate data collection and test execution in order to identify the root cause of an error condition.
Secure	Applications that are used to monitor the environment for indications of unauthorized activity by internal or external entities.
Distribution	Applications that provide the mechanisms needed to transfer and install software within the execution framework. This may include both components that perform initial provisioning as well as tools that distribute updates, patches, new software, and so on.

Metrics

- Percentage of problems identified by the management infrastructure.
- Existence and amount of available performance data (in number of days of history) for components of the execution environment (hardware, storage, network, applications, etc.).

- Number of manual steps required to perform key administration functions, such as adding a user.
- Frequency of system backups.
- Frequency of system restore tests.
- Number of security alerts generated per day / week / month.
- Average number of days to provision a new server.
- Number of diagnostic test routines available for use by OMCM Level 1 support staff.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-5 Element and Resource Management Tools Capabilities Profile

Component	OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Monitor	Ad Hoc	Functional	Effective	Optimized	Optimized
Measure	Ad Hoc	Emerging	Functional	Effective	Optimized
Control	Ad Hoc	Emerging	Emerging	Functional	Optimized
Administer	Ad Hoc	Emerging	Functional	Functional	Optimized
Backup	Emerging	Functional	Effective	Effective	Optimized
Diagnose	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Secure	Emerging	Emerging	Functional	Functional	Optimized
Distributio n	Ad Hoc	Emerging	Emerging	Functional	Optimized

Event and Information Managers

The event and information managers component of the tools framework model consists of applications that manage events and information generated by the lower layers of the model. The focus of the applications at this layer shift from dealing with the measurement and modifications of technical metrics to the management of data and alarms. The functional components at this layer are:

TABLE 10-6 Event and Information Managers

Application	Description
Event Processing	Applications that manage notifications generated by the lower layers (alarms, warnings, etc.). Specific activities include event filtering (discarding of unneeded events), event consolidation (combination or like events), event mapping (transformation of event attributes to standard scheme), and event correlation (parallel processing of events to make inferences concerning the root cause).
Performance Analysis	Applications that are used to process and analyze performance data collected by measuring applications for the purpose of identifying performance bottlenecks.
Capacity Analysis	Applications that are used to process and analyze performance data, along with knowledge or application workload drivers, in order to make predictions about the impact of changes on performance.
Mediation	Applications that bridge the gap between lower layer data collection mechanisms (measurement tools) and external systems used for charge back or billing. Mediation tools provide a means of taking performance data from a wide variety of sources and providing the preprocessing necessary to allow the application of rating and discount parameters by a billing system.

TABLE 10-6 Event and Information Managers *(Continued)*

Application	Description
Notification	Applications that help the process of passing information (alarms, warnings, and so on) to external entities, such as people and other applications. Example: Application that generates pager messages when critical alarm notifications are received.
Configuration Maintenance	Applications that are used to maintain information about the configuration of elements within the execution environment and their relationships to each other. This include applications to manage the configuration management database (CMDB), the definitive hardware store (DHS), and the definitive software library (DSL). The CMDB is a virtual database containing asset and configuration information. The DHS is the storage for field replaceable hardware components. The DSL is the repository of all software master copies.
Report Generation	Applications that are used to process and format performance and event information for use in management review and decision making activities. The focus of reporting at this level is inward towards IT.

Metrics

- Total number of events processed per day.
- Total number of actionable events (requiring action by the operations staff) per day.
- Number and frequency of periodic reports generated for IT management review.
- Number of applications for which a predictive performance analysis model exists.
- Number of hardware field-replaceable unit (FRU) line items maintained by the organization.
- Total number of notifications (pages, emails, and so on) generated per day.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-7 Event and Information Management Tools Capabilities Profile

Component	OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Event Processing	Ad Hoc	Emerging	Effective	Effective	Optimized
Performance Analysis	Ad Hoc	Emerging	Functional	Functional	Optimized
Capacity Analysis	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Mediation	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Notification	Ad Hoc	Functional	Effective	Effective	Optimized
Configuration Maintenance	Ad Hoc	Emerging	Emerging	Functional	Optimized
Report Generation	Ad Hoc	Emerging	Emerging	Functional	Optimized

Service Level Managers

Service level managers are applications that link business requirements (as defined by Service Level Agreements, or SLAs) with the technical status of the execution environment (as determined by the lower layers of the framework). The functional components are:

TABLE 10-8 Service Level Managers

Application	Description
Transaction Generators	Applications that introduce a workload on a specific service and evaluate the level of response received. These synthetic transactions are used to evaluate the service from the perspective of the end user.
KPI Evaluation	Applications that evaluate key performance indicators (KPIs), which may be used as an alternate to—or in conjunction—with transaction generators to assess the availability and performance of a service.
Correlation Engines	Applications that are used to analyze management information and make inferences about the impact of a given event or group of events on a specific service.
SLM Reporting	Applications that provide both real-time and historical reporting on the organization's compliance with published service levels.

Metrics

- Percentage of SLAs for which a transaction test set has been defined and implemented.
- Level of granularity for business impact analysis of failures (service/application, user group, business unit, business process, and so on).
- Average to time notify impacted customers/users of a service level issue.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-9 Service Level Management Tools Capabilities Profile

Component	OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Transaction Generators	Ad Hoc	Emerging	Functional	Optimized	Optimized
KPI Evaluation	Ad Hoc	Ad Hoc	Emerging	Effective	Optimized
Correlation Engine	Ad Hoc	Ad Hoc	Emerging	Emerging	Optimized
SLM Reporting	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Process Workflow Managers

Workflow technology is used to automate the management processes described on the process aspect of the management framework cube. Process and workflow systems include both lower level applications (to perform basic help desk type functions such problem tracking, and change management), as well as more extensive workflow systems that are used to automate more extensive IT operations processes. Also included are implementations that provide end user self service capability.

Criteria

Use the following criteria, along with previously-described criteria, to determine the degree of implementation for the process and workflow management subsystem.

TABLE 10-10 Process and Workflow Management—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Process management is facilitated using available technology that is not necessarily focused on process and workflow management. Example: Using only email and spreadsheets to manage the problem resolution process.
Emerging	• Isolated systems are in place to provide basic help desk functionally. • Automation of process steps, such as notification and escalation, is limited. • Help desk functionality is restricted to help desk staff.
Functional	• Multiple systems are in place to support core management processes (problem, asset, change management). • Basic process steps, such as notification and escalation, are automated. • Functionality is restricted to IT. • Automation of service requests creation by other portions of the management tools infrastructure.
Effective	• Consolidation or integration of multiple systems. • Self service functions are enabled, and functionality is available to non-IT staff. • Two way flow of event information exists between workflow systems and other portions of the management tools infrastructure.
Optimized	• Complex IT processes using workflow technology are extensively automated. • Workflow integration is used to automate activities performed by other portions of the management tools infrastructure. • Functionality is available to business partners and other external organizations.

Metrics

- Number of service requests initiated daily / weekly / monthly.
- Number of service requests closed daily / weekly / monthly.
- Average service time for all classes of service requests.
- Percentage of service requests initiated automatically by the management tools infrastructure.
- Percentage of service requests processed by each level of the support structure, including the percentage of requests met via customer self service mechanisms as well as the various tiers of the organization's support organization.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-11 Process and Workflow Management Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Management Portals

Management portals are collections of applications that provide external entities with access to selected portions of the management framework. Examples: Web interface for reviewing SLM reports, Web or other types of user interfaces for the various tools or applications used by end users to submit requests for service. It should also be possible, and even desirable, to use this portal to expose management information and facilities to people outside of the IT organization.

Criteria

Use the following criteria, along with previously-described criteria, to determine the degree of implementation for the management portal.

TABLE 10-12 Management Portal—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Little or no Web-based access to the management tools infrastructure exists.
Emerging	• Tool specific, Web based access for a subset of the management tools environment is provided by the tools vendor. • Only a subset of each tool's functions can be performed using the Web interface.
Functional	• A majority of the tools infrastructure is available via Web-based access. • Most of each tool's functions can be performed via the web interface.
Effective	• Consolidation of Web access using a common Web infrastructure. • Most of the management tools infrastructure is accessible and most of each tools functions are supported via the Web interface.
Optimized	• True portal functionality includes content and application aggregation and personalization.

Metrics

Not specified in this draft.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-13 Management Portal Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Degree of Visibility

Description

To be effective, the management tools infrastructure must be capable of obtaining information about the environment being managed. In areas that are not visible to the management tools infrastructure, information and notification of critical conditions must be obtained in other ways. Generally, these alternate methods are manual and reactive. The more information that is available concerning the state of the managed environment, the more effective the management infrastructure will be.

Instrumentation provides visibility into the managed environment and can be classified into the following types:

TABLE 10-14 Types of Instrumentation

Application	Description
Agents	Software entities within the execution framework that communicate with management applications in the management framework using a defined protocol and naming scheme for managed objects.
Probes	Special-purpose management entities (hardware and software) that operate in the execution environment to perform specific management functions on behalf of management applications. Probes differ from agents in that probes are stand-alone devices, while agents are generally installed on a component with another purpose.
Ad Hoc Solutions	Scripts and executables that operate in an autonomous fashion on components within the execution framework. These components generally do not communicate with, or act on behalf of, a management application.

Instrumentation components may take the role of sensor (obtaining data from the environment), effector (manipulating the environment), or both.

Degree of visibility refers to the amount of the management environment that is visible to, and accessible by, the management tools infrastructure.

Critical to Quality.

- The organization has defined a specific instrumentation approach that includes selected agent types, supported management protocols, and extensibility mechanisms. Conflicts and overlapping functionality between different agents must be managed.
- Instrumentation is a component of the standard configurations.
- Application development standards include APIs or other mechanisms to support the instrumentation of locally developed applications.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 10-15 Degree of Visibility—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Only a minimal subset of the hardware and network layers is visible.
Emerging	• Critical network and hardware/storage components are visible.
Functional	• A majority of the network and hardware/storage layers of the managed environment is visible. • Key application infrastructure components are visible.
Effective	• The lower three layers of the execution architecture are visible. • A majority of the application infrastructure is visible. • Key applications are visible.
Optimized	• The management infrastructure has complete visibility into the management environment.

Metrics

- Average number of agents per managed system.
- Percentage of problems detected by the management infrastructure.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-16 Degree of Visibility - Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Integration of Components

Description

Because most, if not all, enterprise management infrastructures are built using multiple components from different vendors, these components must be integrate somehow. Integration facilitates operations across management silos and is necessary for organizations engaged in managing to service level agreements that span multiple systems, networks databases, and so on.

Among the approaches available for integrating the different parts of a management system, two categories are generally used:

TABLE 10-17 Component Integration Approaches

Approach	Description
Technology-based Integration	Integration of different components using a technical solution. A number of different options for this type of integration exist, depending on the components being integrated. Examples: Consolidation of events from multiple element managers using product specific event listeners, or direct API calls from an event manager to a help desk system to support the automated creation of problem tickets.
Process-based Integration	Integration of different components via a well defined and documented manual process. Example: Having a help desk operator manually create a trouble ticket for an event seen on the event management console.

Integration of components within the OMCM refers to the degree to which the individual components of the management tools infrastructure are connected to facilitate specific operational processes.

Critical to Quality

- The management tools architecture must specify the required integration points between tools and the methods used to realize the integration.
- In keeping with the idea that the replacement of specific parts of the management tools environment should not invalidate the architecture, components should be loosely coupled so that significant dependencies do not exist between them. Example: Replacement of the event management console should not require major changes in the underlying monitoring systems.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 10-18 Integration of Components—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Components deployed in a silo fashion with little or no defined integration. • Monitoring systems pass alarms to notification systems. • Management data not readily available.
Emerging	• Event management system is primary integration point for event and information management sub systems. • Ad Hoc Integration via informal process. • A small subset of management data is available to subsystems of the tools infrastructure via APIs or other tightly coupled access methods.

TABLE 10-18 Integration of Components—Criteria *(Continued)*

Degree of Implementation	Criteria
Functional	• Service Level Management Tools provide next level of integration. providing a point at which KPIs are captured from lower level sub systems and evaluated. • Formal manual processes used to realize integration between components when needed. • One way integration between the three core layers of the tools infrastructure and the process workflow management subsystem. • Management data available via exposed interfaces for multiple data repositories.
Effective	• Bidirectional integration between process and work flow manager and other parts of the management infrastructure. • Presentation layer integration available for a subset of the management infrastructure. • Components are integrated via well-defined interfaces.
Optimized	• Integration becomes fully realized. • Key integration points are the process and workflow management subsystem, management portal and meta-repository for management data.

Metrics

Not specified in this draft.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-19 Integration of Components - Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Process Automation

Description

The primary purpose for implementing a management tools infrastructure is to automate activities that would otherwise have to be performed manually. A simple example is the activity of reviewing a system log for error conditions. This can be done on a periodic basis by a systems administrator who opens the log file in a text editor and searches for specific types of error messages. Implementation of a monitoring application that performs pattern matching and alerts when necessary relieves the administrator of the requirement to look at the file on a periodic basis. More complex examples include automated recovery actions to specified failure scenarios, customer self-service capabilities (knowledge base, adds, moves changes), and dynamic service provisioning.

Process automation refers to the degree to which processes, policies, and procedures are embedded into, controlled by, and executed by the management tools infrastructure.

Critical to Quality.

- Automation of process requires well understood and well documented procedures.
- A process must be in place to maintain the procedures and associated technical implementation.
- KPIs for each process are identified and tracked so that performance of the automated process is understood.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 10-20 Process Automation—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Little or no automation of processes exists.
Emerging	• Some automation exists for basic administrative activities (user maintenance, and so on). • Limited automated actions are based on alarms or other conditions.
Functional	• Repetitive tasks are identified and automated (provisioning, user maintenance, and so on). • Key process activities (escalations, notifications, routing of work) are automated.
Effective	• Automation is extended to include customer self service capabilities. • IT process is extensively automated. • Recovery activities are extensively automated.
Optimized	• High value activities (recovery, dynamic provisioning, diagnostics) are fully automated.

Metrics

- Percentage of user service requests satisfied through self service mechanisms.
- Number of IT processes implemented and controlled by a process workflow management tool.
- Availability of metrics that quantify the process execution.
- Cycle time (request to completion) for critical activities, such as user adds and service provisioning.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

TABLE 10-21 Process Automation - Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Ad Hoc	Emerging	Functional	Optimized

Effectiveness of the Implementation

Description

Like any other business investment, organizations need to justify the expenditures towards improving operational capability by realizing some value for the investment. For the purpose of the OMCM, we define investment in a tools infrastructure as *organizational effort needed to implement and maintain the infrastructure.* This effort is measured by the expenditure of capital, human effort, and other organizational resources.

We define value for a tools infrastructure as benefits received by the organization through:

- Avoidance of risk and costs associated with unavailability of services.
- Cost savings as the result of efficiency improvements in the management of the IT infrastructure.
- Revenue gains by reducing or eliminating IT operations as a bottleneck in the introduction of new services.
- Revenue gains enabled through new product offerings made possible by the IT management infrastructure.
- Effectiveness of the implementation refers to the value received by the organization as a function of the investment.

Critical to Quality

- The organization should have a budget for the implementation and maintenance of the management tools infrastructure.
- Metrics to quantify and measure IT operational efficiency, and contributions to profitability, should be identified and tracked. Investments in the management infrastructure should be justified by an expected improvement in one or more of the metrics.
- Efforts to avoid capital expenditures by developing local solutions should be discouraged by the organization. Locally developed tools eventually cause maintenance and extensibility problems as the organization matures.

Criteria

Use the following criteria to determine the degree of implementation.

TABLE 10-22 Effectiveness of the Implementation—Criteria

Degree of Implementation	Criteria
Ad Hoc	• Little or no value is realized by the organization. • High percentage of locally developed tools have increasing maintenance requirements.
Emerging	• Minimal value is provided to the organization. • Shift to commercial off the shelf (COTS) technology is used to mitigate maintenance and extensibility issues.
Functional	• The management infrastructure becomes necessary to conducting IT business. • Value from the management infrastructure is justified by quality of service.
Effective	• IT realizes productivity gains and cost savings from the management infrastructure. • The management infrastructure is core to the delivery of IT services. • The business value is released from the management infrastructure. • Deployment and maintenance costs of the IT management infrastructure are justified by cost and productivity improvements.
Optimized	• Management infrastructure is required to deliver the business. • High value is realized.

Metrics

- Annual budget for enterprise management tools.
- Full-time employee (FTE) for IT operations.

Capabilities Profile

The following degrees of implementation are expected at each capability level of the OMCM.

Figure 1 Effectiveness of the Implementation—Capabilities Profile

OMCM Level 1 Crises Control	OMCM Level 2 IT Component Management	OMCM Level 3 IT Operations Management	OMCM Level 4 IT Service Management	OMCM Level 5 Business Value Management
Ad Hoc	Emerging	Functional	Effective	Optimized

Summary of the Tools Capabilities Profile

The following table summarizes the degree of implementation profile for each OMCM level of the tools aspect.

TABLE 10-23 Capabilities Profile Summary of the OMCM Tools Aspect

Category	Level 1 Crises Control	Level 2 IT Component Management	Level 3 IT Operations Management	Level 4 IT Service Management	Level 5 Business Value Management
Specification of Tools Architecture	Ad Hoc	Emerging	Functional	Effective	Optimized
Implementation of Functional Components - Monitor	Ad Hoc	Functional	Effective	Optimized	Optimized
Implementation of Functional Components - Measure	Ad Hoc	Emerging	Functional	Effective	Optimized
Implementation of Functional Components - Administer and Control	Ad Hoc	Emerging	Functional	Functional	Optimized
Implementation of Functional Components - Backup	Emerging	Functional	Effective	Effective	Optimized
Implementation of Functional Components - Diagnose	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Implementation of Functional Components - Secure	Emerging	Emerging	Functional	Functional	Optimized
Implementation of Functional Components - Distribution	Ad Hoc	Emerging	Emerging	Functional	Optimized
Implementation of Functional Components - Event Processing	Ad Hoc	Emerging	Effective	Effective	Optimized

TABLE 10-23 Capabilities Profile Summary of the OMCM Tools Aspect *(Continued)*

Implementation of Functional Components - Performance Analysis	Ad Hoc	Emerging	Functional	Functional	Optimized
Implementation of Functional Components - Capacity Planning	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Implementation of Functional Components - Mediation	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Implementation of Functional Components - Notification	Ad Hoc	Functional	Effective	Effective	Optimized
Implementation of Functional Components - Configuration Maintenance	Ad Hoc	Emerging	Emerging	Functional	Optimized
Implementation of Functional Components - Report Generation	Ad Hoc	Emerging	Emerging	Functional	Optimized
Implementation of Functional Components - Transaction Generators	Ad Hoc	Emerging	Functional	Optimized	Optimized
Implementation of Functional Components - KPI Evaluation	Ad Hoc	Ad Hoc	Emerging	Effective	Optimized
Implementation of Functional Components - Correlation Engine	Ad Hoc	Ad Hoc	Emerging	Emerging	Optimized
Implementation of Functional Components - SLM Reporting	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Implementation of Functional Components - Process Workflow Managers	Ad Hoc	Emerging	Functional	Effective	Optimized
Implementation of Functional Components - Management Portal	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Degree of Visibility	Ad Hoc	Emerging	Functional	Effective	Optimized

TABLE 10-23 Capabilities Profile Summary of the OMCM Tools Aspect *(Continued)*

Integration of Components	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Process Automation	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Effectiveness of the Implementation	Ad Hoc	Emerging	Functional	Effective	Optimized

3

Part 4—Conclusion

This part of the document does provides a conclusion and additional resources. It includes the following chapters:

- Chapter 11, “Application of the OMCM”
- Chapter 12, “Resources for More Information”
- Chapter 13, “About the Authors”

11

Application of the OMCM

In this document, we have provided an overview of a management framework that describes the components of IT operational capability, and an evolutionary model that describes how organizations should realize this framework over time. This chapter provides some brief guidance on use of the OMCM. It contains the following sections:

- Assessment and Scoring
- Vendor Application

The OMCM is applicable to a variety of activities that are focused on improving operational capability. We see its main value as being a communications tool that allows an organization to clearly describe both its current and desired states of operational readiness. It also serves to help identify targets for short term and long term investment.

For vendors like Sun, this model provides a means to segment the customer market and target products and services based on the current operational capability of a customer. It is our contention that the needs of a customer at OMCM Level 2 are significantly different from the needs of an OMCM Level 4 customer.

Assessment and Scoring

The most obvious application of the OMCM is its use as an assessment vehicle to help organizations benchmark their level of operational capability as a first step in an improvement effort. Part 2, "Sun IT Management Framework," of this document was written to facilitate a lightweight assessment. More detailed assessments are possible using the wealth of ITIL, CMM, and other available collateral to drill down into the details of the specific areas. Sun Microsystems has a number of vehicles to assist in this effort, such as ITIL assessments and the SunReady Availability Assessment. The goal is to develop a snapshot of the organization that provides input into the remediation plan.

This document does not specify how to arrive at a score for a given organization. There is a natural desire for people to want a grade as a measure of how well they are doing. Although it is possible to provide such a grade using the OMCM, we have deliberately left this as an exercise for the implementer, for two reasons:

- We believe that the focus of OMCM application should be on the state of individual components, not on the overall score. The fact that an organization decides it is a OMCM Level 2 is less useful than the identification of the people, process, and tools areas that are not implemented to the degree necessary to meet the desired OMCM level. Targeted diagnosis helps focus investment for the organization.
- We believe any implementation of the OMCM must take into account the political realities of the organization. By not specifying a scoring approach, we give implementers the flexibility to tailor the message so that it is most effective for driving the desired organizational behavior.

Although we do not offer a prescriptive scoring methodology, we do provide a couple of generalized approaches.

The following table shows the results of a process assessment performed by Sun Microsystems for one of its customers. The degree of implementation for each component is highlighted.

TABLE 11-1 OMCM Process Aspect Assessment Results

Process	Sub-Process	OMCM Level 1 Profile	OMCM Level 2 Profile	OMCM Level 3 Profile	OMCM Level 4 Profile	OMCM Level 5 Profile
Create IT Services	Service Level Mgt.	Ad Hoc	Ad Hoc	Emerging	Functional	Optimized
Create IT Services	Availability Mgt.	Ad Hoc	Emerging	Functional	Effective	Optimized
Implement IT Services	Release Mgt.	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Deliver IT Services	Capacity Mgt	Ad-Hoc	Emerging	Functional	Effective	Optimized
Deliver IT Services	Incident Mgt.	Ad-Hoc	Emerging	Functional	Optimized	Optimized
Deliver IT Services	Service Desk	Ad-Hoc	Ad-Hoc	Functional	Effective	Optimized
Improve IT Service	Problem Mgt.	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized
Improve IT Service	Sun^{SM} Sigma	Not Assessed				
Control	IT Financial Mgt.	Ad-Hoc	Emerging	Functional	Optimized	Optimized
Control	Configuration Mgt.	Ad-Hoc	Ad-Hoc	Emerging	Effective	Optimized
Control	Change Mgt.	Ad-Hoc	Emerging	Functional	Effective	Optimized
Protect	IT Service Continuity	Ad-Hoc	Ad-Hoc	Emerging	Functional	Optimized

Two potential approaches may be taken to determine the OMCM level from these results.

- One approach is an extension of the strict ordering concept introduced in Chapter 2, “Introduction.” Strict ordering means that the organization cannot achieve a given level unless it has satisfied the requirements of that level and all

of the previous levels. Under this criteria, the organization represented in the above table would be considered at OMCM Level 1. This approach is particularly useful when certification to a certain capability is required.

- Another approach is to determine the center of mass for the sum of the categories. The idea here is that the organization's OMCM level is determined by assessing the fit between the customer results and the OMCM level profile. For example, if a majority of the components have a degree of implementation that brings them to OMCM Level 4, with a couple trailing and a couple at OMCM Level 5, then the organization would be OMCM Level 4. In the case of our sample company assessment, the results seem to indicate an OMCM Level 2 organization. The case may even be made that they are at OMCM Level 3 based on the number of processes that have the necessary degree of implementation.

Regardless of the approach taken, and the final grade, the real value in the above assessment is the identification of capacity, problem, and configuration management areas requiring attention.

Vendor Application

As we stated above, service providers, ISVs, and other vendors can use the OMCM to segment their customers and categorize their offerings. The table below shows an example segmentation along with suggested focus areas for offerings. The goal is to tailor the solution to the customer capability level.

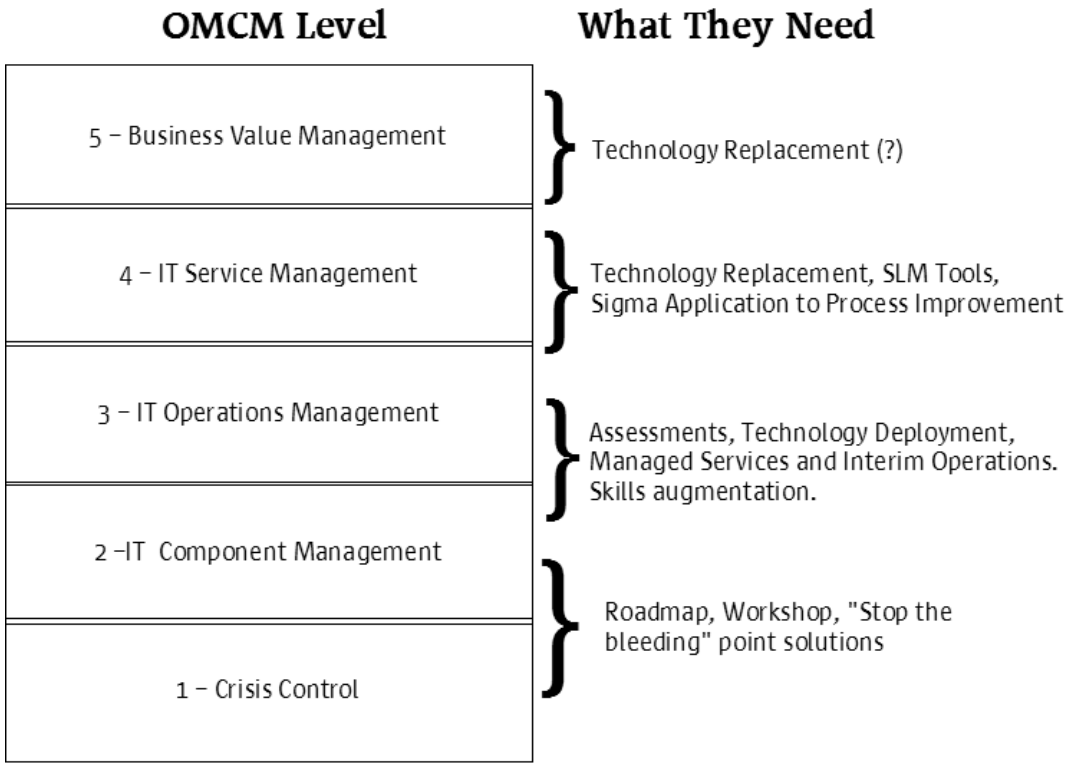

FIGURE 11-1 OMCM Based Remediation Approaches

For example, it has been our experience that organizations at levels one and two will need help in stabilizing the environment before they are able to support longer term efforts to improve capability. For these organizations, appropriate services could provide additional on site expertise (staff augmentation or management services) and tools with rapid implementation times that provide basic monitoring.

12

Resources for More Information

This chapter describes additional information on operational capability and other topics discussed in this document. For more information about Sun Microsystems, Inc., see the following URL: http://www.sun.com

Service Management and IT Process Links

TABLE 12-1 Service Management and IT Process Resources

Organization	URL
IT Service Management Forum home page	http://www.itsmf.com
IT Service Management Forum US home page	http://www.itsmf.net
Information Systems Audit and Control Organization. This organization maintains the COBIT standard	http://www.isaca.org
Home page for the BS1500 IT Service Management Standards	http://www.bs15000.org.uk
Software Engineering Institute. The SEI has a number of ongoing maturity model efforts.	http://www.sei.cmu.edu/sei-home.html

Management Tools Vendors

TABLE 12-2 Management Tools Vendors

Vendor	URL
BMC Software	http://www.bmc.com
Aprisma	http://www.aprisma.com
Micromuse	http://www.micromuse.com
Teamquest	http://www.teamquest.com/
Halcyon Monitoring Solutions	http://www.halcyoninc.com/

13

About the Authors

This chapter provides more information about the authors of this document.

Edward Wustenhoff

Edward Wustenhoff is currently an IT Management Strategist in the Global Datacenter Practice of Sun Client Solutions. He has more than 15 years' experience in networked computer systems and data center management. During the past nine years at Sun, he has been involved with Sun's technologies and Datacenter Best Practices. In one of his previous roles at Sun, he managed the Enterprise Management Practice, where he advised Sun's customers about Datacenter Management best practices, tools selection, and deployment strategies.

At Applied materials. Mr. Wustenhoff held several datacenter operations positions. Above all, he has two children, Anneke and Christiaan, and a wonderful wife, Therese, who have taught him more about how to develop strategies for change and receive honest feedback, than any other experience.

Michael J. Moore

Michael. Moore is currently a Solution Architect in the Global Data Center Practice of Sun Client Solutions. Mr. Moore has over 20 years of experience in the design and operations of IT systems and networks. During this time, his focus has been on technologies and best practices for systems and network management. Recent work has included development of a IT management meta-framework for use in the design of enterprise management solutions, and the development of a operations capabilities maturity model for IT organizations. Mr. Moore's experience also includes the development and implementation of enterprise management solutions using a wide range of products; and over 10 years of IT operations experience in both the military and commercial sectors. He is a Certified Micromuse Consultant and a Certified Aprisma Spectrum Engineer.

Dale H. Avery

Dale Avery is currently a Practice Development Manager for Sun Educational Services. Mr. Avery has over 25 years' experience in the technology sector, including application and system software design and development. He has also managed the development and deployment of IT applications. Mr. Avery specializes in the areas of efficiency, use of best practices, and continuous improvement. He has managed organizations that provided development support to software and hardware application vendors. He has been responsible for training and developing people in organizations. Most recently, he participated in the development of the People Aspect in Sun's Operational Maturity Capability Model. Mr. Avery holds a BS degree in Information Technology and is certified in Prince2.

Index