Best Practice Insights

Focus On: ITIL® Service Transition

Updated for ITIL 2011

bmcsoftware

This publication has been revised to bring the content up-to-date with IT Infrastructure Library® (ITIL®) 2011 by Anthony Orr. Orr is Director of Service Management and works within the Office of the CTO at BMC Software. He is one of the authors for the ITIL 2011 update and a senior ITIL examiner for APMG. Orr has more than 30 years of information technology experience.

We greatly appreciate the contributions of the following individuals to the original version of this publication:
Dag Blokkum
Ken Turbitt
Frederieke C. M. Winkler Prins

Note to Readers

This booklet highlights key elements of the ITIL *Service Transition* publication and includes commentary on important concepts from BMC ITIL experts. BMC commentary is highlighted in blue text.

This publication has been revised to bring the content up-to-date with IT Infrastructure Library® (ITIL®) 2011 by Anthony Orr. Orr is Director of Service Management and works within the Office of the CTO at BMC Software. He is one of the authors for the ITIL 2011 update and a senior ITIL V3 examiner for APMG. Orr has more than 30 years of information technology experience.

We greatly appreciate the contributions of the following individuals to the original version of this publication:
Dag Blokkum
Ken Turbitt
Frederieke C. M. Winkler Prins

Note to Readers

This booklet highlights key elements of the ITIL *Service Transition* publication and includes commentary on important concepts from BMC ITIL experts. BMC commentary is highlighted in blue text.

Foreword

Organizations are constantly changing, and this can have a significant impact on how the business, the service provider, and their personnel all work. The introduction or decommissioning of a service often requires significant changes that need to be managed and delivered through the service lifecycle. Where there is major change, there will be complexity and risk. Many organizations deliver significant change through formal projects; however, many projects fail to include the full service management, operational, and functional requirements. This often leads to project failure or additional cost and risk.

Service transition sits at the center of the IT Infrastructure Library® (ITIL)® lifecycle structure. Service design supplies its inputs, and service operation receives its outputs — which are usable services. Successful service transition requires the effective application of change management, quality assurance, and risk management at each stage through the service transition process to establish and confirm progress against current requirements — not just for one service, but across all services in transition.

Service transition works with projects to establish assurance of the actual and expected service deliverables. It covers the assessment of the predicted performance of a service against the actual performance and management of any deviation and associated risks prior to service acceptance. Adopting service transition practices can enable service improvement and increase an organization's service management capability by ensuring that the introduction, deployment, transfer, and decommissioning of new or changed services are consistently well managed.

Shirley Lacy
Managing Director, ConnectSphere
Co-author of the ITIL *Service Transition* publication,
by the Office of Government Commerce (OGC)

Table of Contents

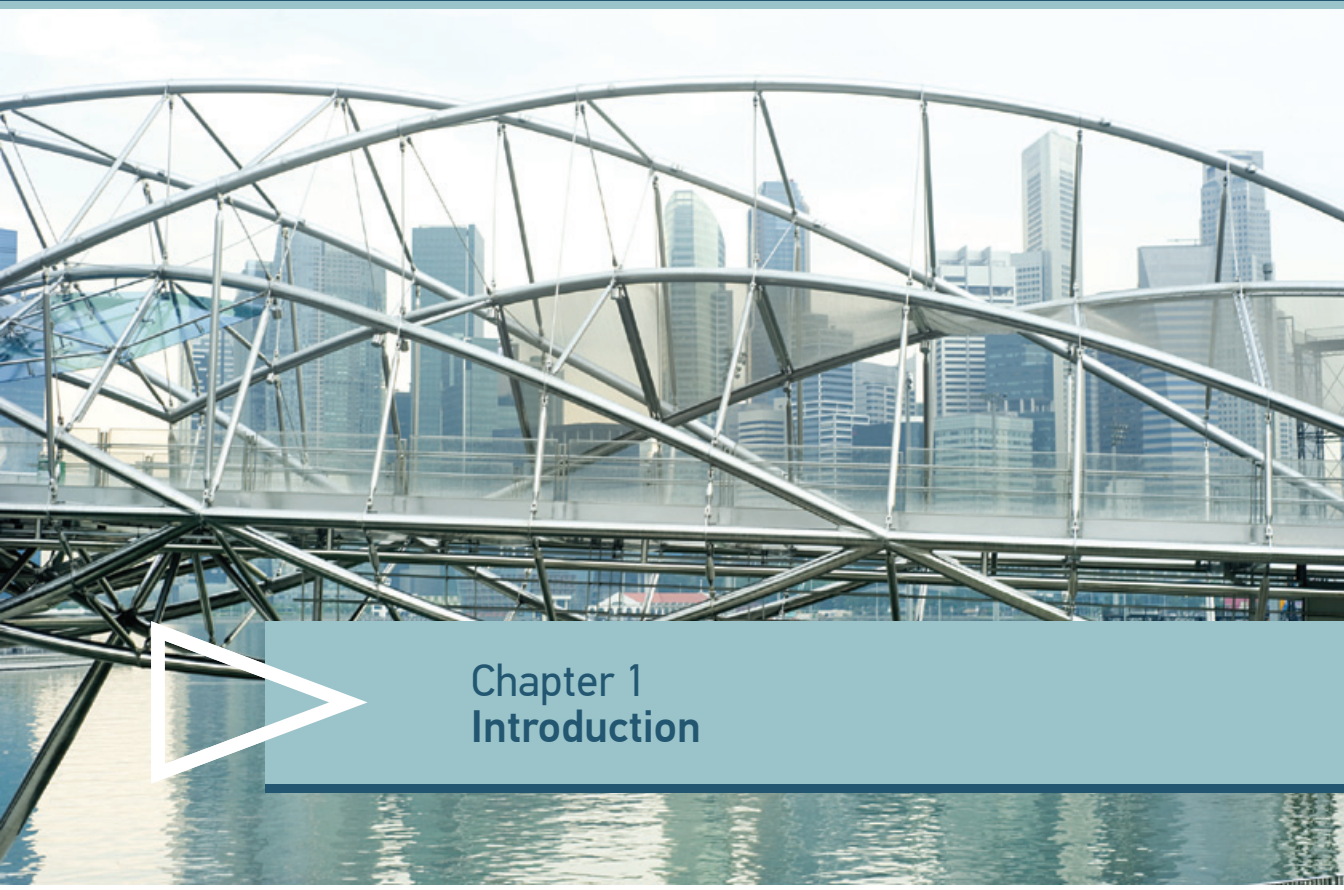
Foreword

Organizations are constantly changing, and this can have a significant impact on how the business, the service provider, and their personnel all work. The introduction or decommissioning of a service often requires significant changes that need to be managed and delivered through the service lifecycle. Where there is major change, there will be complexity and risk. Many organizations deliver significant change through formal projects; however, many projects fail to include the full service management, operational, and functional requirements. This often leads to project failure or additional cost and risk.

Service transition sits at the center of the IT Infrastructure Library® (ITIL)® lifecycle structure. Service design supplies its inputs, and service operation receives its outputs — which are usable services. Successful service transition requires the effective application of change management, quality assurance, and risk management at each stage through the service transition process to establish and confirm progress against current requirements — not just for one service, but across all services in transition.

Service transition works with projects to establish assurance of the actual and expected service deliverables. It covers the assessment of the predicted performance of a service against the actual performance and management of any deviation and associated risks prior to service acceptance. Adopting service transition practices can enable service improvement and increase an organization's service management capability by ensuring that the introduction, deployment, transfer, and decommissioning of new or changed services are consistently well managed.

Shirley Lacy
Managing Director, ConnectSphere
Co-author of the ITIL *Service Transition* publication,
by the Office of Government Commerce (OGC)



Chapter 1
Introduction

Think of the steps in service management as similar to the steps in launching a space mission. Perhaps your strategy is to be the first nation to conduct scientific research by landing astronauts on Mars. In the strategy phase, you define the mission requirements as well as acquire all the needed approvals and funding.

The next steps are to figure out what research is needed, assemble the best team to do it, and design a spacecraft that will safely travel to Mars and home again. In the design phase, you acquire all the technical expertise, requirements, and plans to architect and design the spaceship. Your team builds a new spacecraft to specifications. Some existing systems or designs may be reused, with modifications.

As you get closer to launch (similar to the transition stage in service management), you test everything to make sure it's working perfectly. If it isn't, the launch is postponed until the problem can be fixed. The fix might require a pullback of some services or further modifications to equipment that had seemed to be in perfect order. You keep the crew and all the teams informed during the entire process. When everyone can be confident that everything is working properly, the spacecraft will leave the launch pad, and the mission will be in its operations phase.

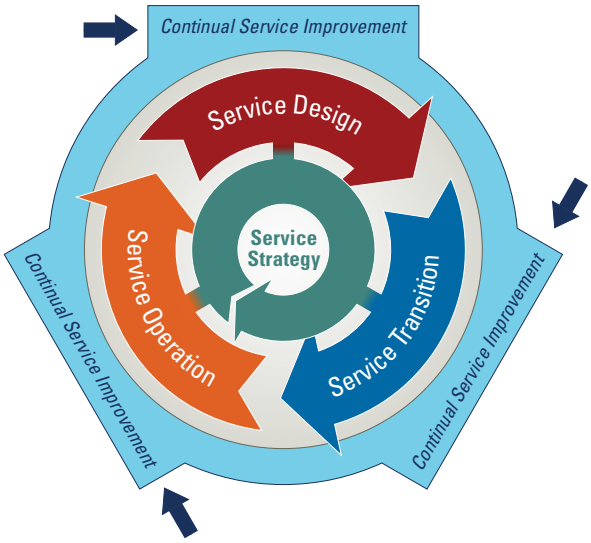


Figure 1. ITIL Service Management Lifecycle

The Service Management Lifecycle

Figure 1 illustrates the ITIL service management lifecycle. The goal of service strategy is to design, develop, and implement service management as both an organizational capability and a strategic asset. Service design focuses on ensuring that the IT service assets offered to the business fulfill the objectives of the business.

In service transition, the focus is on delivering a smooth ride from design and development to value realization in operations. Service operation strives to effectively manage operational priorities, such as the availability of the IT services provided to the business; to optimize the use of existing infrastructure; and to support the IT users in resolving issues.

Improving the quality of existing IT services is the heart of the value delivered by continual service improvement, which, according to ITIL, "ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes."[4] This stage represents the loop back to improvements in strategy, design, transition, and operations, as it is a continual learning process.

Why Read *Service Transition*?

Your IT team constantly plans new services or service changes, then must release them into the service environment. The *Service Transition* publication will provide you with best-practice guidelines to help you do just that. The beauty of these guidelines is that, while giving you benchmarks for the basics, they allow room for customization according to your own business needs. As you plan, build, test, evaluate, and deploy, you can make changes to minimize the risk of failure or business disruption based on your own, unique situation.

> Service transition helps manage risk and ensure stakeholder readiness for your new, changed, or retired service.

4 Ibid. See *Continual Service Improvement*.

Service transition is helpful in a variety of situations, including the following:

- Changing or adding a service isn't as simple as it might sound. Much complexity is involved in making sure all systems work together seamlessly.
- One size does not necessarily fit all. Your IT team may need to adapt and innovate.
- When you must make a change to an existing supplier, service, or service provider, service transition can help ease the business into the switch.
- Replacing systems, hardware, and applications is more complicated than it first appears. There are critical dependencies to consider: old and new software may not "talk" to each other, people may require retraining, and your processes may need to be updated. Each action has its own repercussions and costs. Service transition can help you predict the effects and minimize the risk of failure during the changeover.
- Transferring services from one provider to another may have a ripple effect in ways you might not anticipate. But, once again, if you follow the service transition guidelines, the change will be less painful and your success rate will increase.
- When the service management capability (people, processes, projects, the organization, or how it all works) of an internal or external service provider changes, service transition can help your organization adjust and adapt.

Service transition also provides early life support in the beginning of implementation, until successful operation is ensured and the requirements set forth in the service strategy stage are realized. Service transition helps manage risk and ensure stakeholder readiness for your new, changed, or retired service.

Summary

The ITIL lifecycle approach consists of looking at every service from its conception through operation and then retirement. Most organizations start with continual improvement, but if the organization is new, then strategy is the starting place. A continual improvement initiative supports strategy, design, transition, and operations. To address the strategy, first determine your market and, specifically, the services you want to provide. Eventually, you will build the service, improve the service, test it, release it, then put it into or take it out of operation for value realization. ITIL has formalized best practices for the full lifecycle of a service, yet allows for innovation and adaptation to each organization's unique circumstances.

The service transition part of the lifecycle focuses on how to roll out new or changed/modified/enhanced/retired services to the business, managing the change until it's ready for release and deployment, then following it into successful operation. The objective is to minimize risk and provide the knowledge needed for decision support in transitioning the services to a desired state — *and* to do it all in a timely and cost-effective manner.

Bringing this scenario back to IT, in service transition, you'll conduct adequate testing and have the opportunity to pull back any services or modifications that won't deliver the value you expected them to. You'll be able to make fixes to prevent disaster. And you'll ensure a smooth transition by letting your stakeholders know what's happening and how it will affect them. As you implement your project, you'll provide essential support and oversight to make sure it has a successful launch. The *Service Transition* publication provides many more details about this process.

BSM creates a holistic, customer-centric view that allows IT to effectively manage from the business customer's perspective, both increasing the quality of the services delivered and decreasing the cost associated with service delivery.

An Overview of Service Transition

In the ITIL V3 approach, IT processes are part of a lifecycle, or continuum, in which IT services are viewed as business assets. The purpose of service transition is to maximize the business value of the IT services your organization provides, manage risk, and manage knowledge for decision support.

By following the guidance in *service transition*, you'll be able to manage necessary changes in the broader service environment. You'll have the big picture that allows you to make those changes with an awareness of their potential impact on the rest of your IT services, on the business, and on other factors.

Service transition considers more than just one project; it supports all services that are currently in transition. What's more, it provides support for these projects beyond initial implementation through the early stages of service operation.

IT as a Service Provider

IT is now viewed as a service to the business — one that creates value to the business and runs like a business itself. IT is a business asset that provides capabilities and resources to support business outcomes, such as business efficiency, business growth, and business transformation.

A large telecommunications company provides an excellent example of the various roles IT can play. When the company first released cell phones, IT performed a single-service function: enabling customers to make calls. Over the years, consumers and the business have demanded more. Today, cell phones are smarter and provide a host of services to the end consumer. IT has developed multiple capabilities that have transformed the business to participate in new markets and allow customers to make purchases, take pictures, access email, and perform many other activities. In this company, IT is actively enabling and growing the top and bottom lines, providing a complex range of services that bring revenue to the business and value to its customers.

A Customer-Centric View

Just as IT service management changes the IT focus from the activities and complexity associated with managing IT from an infrastructure-centric approach, Business Service Management (BSM) allows IT organizations to get a clear view of the relationships among the infrastructure elements and the tangible business processes and key metrics they support.

BSM is defined by ITIL as "the management of business services delivered to business customers. Business service management is performed by business units."[1]

Imagine being able to seamlessly identify a business service and understand how the performance of the underlying infrastructure affects the business-critical aspects of the end service that you provide. BSM creates a holistic, customer-centric view that allows IT to effectively manage from the business customer's perspective, both increasing the quality of the services delivered and decreasing the cost associated with service delivery.

A Common Vocabulary

Let's start the discussion of the service management lifecycle with two terms defined by ITIL. To find these and other definitions, refer to the ITIL glossary (http://www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx). For more complete discussions of these terms, see the *Service Transition* publication.

- An *IT service* is "a service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement. Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services."[2]
- "*Service management* is a set of specialized organizational capabilities for providing value to customers in the form of services."[3] IT services are aligned to, and support, business needs. A service management approach helps make the business more successful, reduces disruption, and lowers costs, while increasing revenue.

1 *ITIL English 2011 Glossary,* http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx. See *Business Service Management.*

2 Ibid. See *IT Service.*

3 Ibid. See *Service Management.*

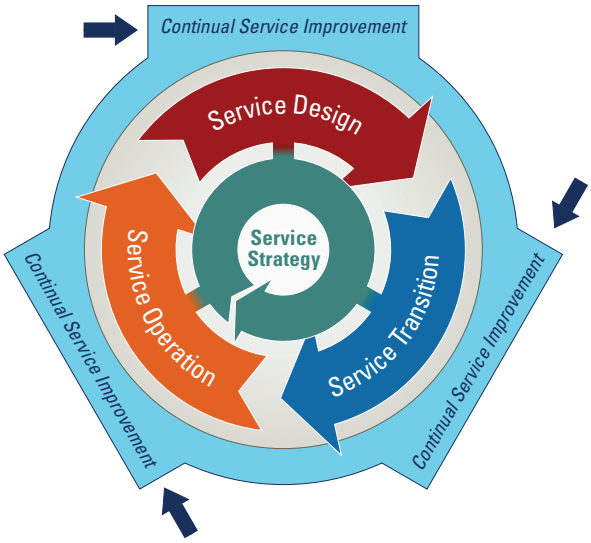


Figure 1. ITIL Service Management Lifecycle

The Service Management Lifecycle

Figure 1 illustrates the ITIL service management lifecycle. The goal of service strategy is to design, develop, and implement service management as both an organizational capability and a strategic asset. Service design focuses on ensuring that the IT service assets offered to the business fulfill the objectives of the business.

In service transition, the focus is on delivering a smooth ride from design and development to value realization in operations. Service operation strives to effectively manage operational priorities, such as the availability of the IT services provided to the business; to optimize the use of existing infrastructure; and to support the IT users in resolving issues.

Improving the quality of existing IT services is the heart of the value delivered by continual service improvement, which, according to ITIL, "ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes."[4] This stage represents the loop back to improvements in strategy, design, transition, and operations, as it is a continual learning process.

Why Read *Service Transition*?

Your IT team constantly plans new services or service changes, then must release them into the service environment. The *Service Transition* publication will provide you with best-practice guidelines to help you do just that. The beauty of these guidelines is that, while giving you benchmarks for the basics, they allow room for customization according to your own business needs. As you plan, build, test, evaluate, and deploy, you can make changes to minimize the risk of failure or business disruption based on your own, unique situation.

> Service transition helps manage risk and ensure stakeholder readiness for your new, changed, or retired service.

4 Ibid. See *Continual Service Improvement*.

Service transition is helpful in a variety of situations, including the following:

- Changing or adding a service isn't as simple as it might sound. Much complexity is involved in making sure all systems work together seamlessly.
- One size does not necessarily fit all. Your IT team may need to adapt and innovate.
- When you must make a change to an existing supplier, service, or service provider, service transition can help ease the business into the switch.
- Replacing systems, hardware, and applications is more complicated than it first appears. There are critical dependencies to consider: old and new software may not "talk" to each other, people may require retraining, and your processes may need to be updated. Each action has its own repercussions and costs. Service transition can help you predict the effects and minimize the risk of failure during the changeover.
- Transferring services from one provider to another may have a ripple effect in ways you might not anticipate. But, once again, if you follow the service transition guidelines, the change will be less painful and your success rate will increase.
- When the service management capability (people, processes, projects, the organization, or how it all works) of an internal or external service provider changes, service transition can help your organization adjust and adapt.

Service transition also provides early life support in the beginning of implementation, until successful operation is ensured and the requirements set forth in the service strategy stage are realized. Service transition helps manage risk and ensure stakeholder readiness for your new, changed, or retired service.

Summary

The ITIL V3 lifecycle approach consists of looking at every service from its conception through operation and then retirement. Most organizations start with continual improvement, but if the organization is new, then strategy is the starting place. A continual improvement initiative supports strategy, design, transition, and operations. To address the strategy, first determine your market and, specifically, the services you want to provide. Eventually, you will build the service, improve the service, test it, release it, then put it into or take it out of operation for value realization. ITIL V3 has formalized best practices for the full lifecycle of a service, yet allows for innovation and adaptation to each organization's unique circumstances.

The service transition part of the lifecycle focuses on how to roll out new or changed/modified/enhanced/retired services to the business, managing the change until it's ready for release and deployment, then following it into successful operation. The objective is to minimize risk and provide the knowledge needed for decision support in transitioning the services to a desired state — *and* to do it all in a timely and cost-effective manner.

Chapter 2
Service Management as a Practice

Service management gives customers value through IT services. The resources themselves have little value until they are transformed into services.

Today, IT has adopted a service-oriented approach to providing value to the business and to its customers, both internal and external. For example, once an application is installed, IT will maintain the application and its supporting infrastructure to ensure it is operating as the business requires. This service orientation has its own challenges, as outsourcing and shared services increase the demand for service providers and service management.

Two Sides of a Service

Each service can be viewed in two ways. As you might expect, the business focuses on the service's desired business outcome, or the utility of the service. For example, many companies outsource their payroll to a financial management company. The company isn't really purchasing the service; it is buying the outcome, which is the on-time processing of paychecks for its employees.

How to Measure Service Transition Success

The business adage, "You must measure what you treasure," is equally true with service transition. Items that you care about need to be measured. If you don't measure your progress, you can't manage it. If you can't manage it, you can't improve it.

Following are some metrics that can help you achieve the goals of service transition:

- How many service transition plans effectively deliver the results anticipated by business units?
- What percentage of all changes to services are managed by service transition?
- What are the change success rates of projects that use service transition?
- Does adherence to service transition reduce outages and negative business impact?
- Are unauthorized changes reduced by service transition planning?
- What are the actual resources used in a deployment versus those predicted in service design?
- Are incidents, problems, and failed changes trending down?
- Are project budgets tracking with predicted values?
- What overhead does using service transition add to projects?

The Policy Angle

A formalized policy is necessary to ensure the success of your service transition efforts. Your IT management team should define and document the objectives and accountability for the service transition activities in your organization. This policy should fit with your existing system of controls and your overall process and governance framework.

The *Service Transition* publication describes several basic policies of service transition, along with lists of principles and best practices associated with them. These include the importance of defining and implementing a formal service transition policy, making sure that service transition is used whenever a service changes, using a common framework, providing for the transition of knowledge, correcting your course as needed, ensuring quality, and more.

Summary

Due to the changing, competitive nature of business today, the requirements for value (utility and warranty) are always increasing. You constantly need higher performance and fewer constraints so you can maintain your customers. Customers of today are no longer loyal. They may switch to the lowest-cost benefit provider or a better offer in the blink of an eye. Organizational governance, policies, and performance optimization are important principles for service value. You must be on a never-ending quest to improve both utility and warranty. Following the ITIL guidance and implementing BSM will help you accomplish that goal.

The other side of the service includes the many back-office processes and systems used to deliver and warrant the service to the customer. In most cases, the company doesn't want to buy or operate a complex IT infrastructure; all it really wants is the desired outcome of the service that its business requires.

The service provider aggregates all of the clients' needs and builds a shared process, a solution, and a control infrastructure to deliver the desired outcome. This aggregation allows the service provider to achieve an economy of scale, while the clients are not exposed to the full cost and risk associated with managing the infrastructure and applications.

Chapter 2 introduces definitions that provide a basis for the ITIL framework and presents concepts that are essential to service management success. Significant points stressed in this chapter are value creation, the importance of organizing for service management, and the service lifecycle. The overriding message in this chapter is to think about how the services you provide are architected in the context of how service value is created and realized for your customers. Please refer to the ITIL glossary[5] for the definitions of the following terms: *service management*, *customers*, *users*, *suppliers*, *service*, *utility*, *warranty*, and *process*.

> Everyone in the organization should be considered a stakeholder for service management.

Stakeholders

Everyone in the organization should be considered a stakeholder for service management. Service is everyone's responsibility, no matter what role they play or how they play the role to deliver and support services for their customers.

External stakeholders — the customers, users, and suppliers — also should be considered. These stakeholders and the organizational stakeholders are an example of the agency principle.

Utility of Service

Customers want to achieve business outcomes by using services that are fit for their purpose. The utility of a service must support customers' performance or remove a constraint. Customers can become very frustrated with a service that is fit for their purpose but lacks sufficient warranty for their use.

5 Ibid.

Warranty of Service

This chapter provides guidance on warranty of service, which you can communicate to customers in terms of commitments to the *availability*, *capacity*, *continuity*, and *security* of the utilization of services.

- *Availability* means that the customer can use your service under the terms and conditions you have mutually agreed upon.
- *Capacity* ensures that the customer will be able to utilize the service at a specified level of business activity or that demand will be fulfilled at a specified quality level.
- *Continuity* guarantees that the customer will be able to use the service even if you experience a major failure or other unexpected event.
- *Security* means that the customer's utilization of services will be free of specific risks.

Many of the services IT provides are considered commodities. You create a competitive advantage when you are able to deliver a certain level of warranty to your customers.

Customers, both internal and external, need to be confident that you can effectively and consistently support their business strategies. Since service providers are constantly matching others' service offerings, you must constantly improve your value proposition to stand apart. Use one or more of the service management processes to drive these improvements.

You create a competitive advantage when you are able to deliver a certain level of warranty to your customers.

Service Assets

According to ITIL, resources and capabilities are types of assets that organizations can use to create value for their customers. *Resources* are direct inputs to produce a service, while *capabilities* are the organization's abilities to utilize resources to create value. You can create differentiation and retain customers by developing distinctive capabilities that are difficult for your competitors to replicate.

Processes

Processes have inputs or triggers, defined actions and activities, and an output or specific results. Processes also have metrics and deliver primary results to a customer in the form of services. Capabilities and resources within or external to the organization enable processes. Processes should follow enterprise governance standards, and policy compliance should be built into them. Governance ensures that the required processes are executed correctly. Processes are executed by people and sometimes are enabled by technology implementations. When processes are collaborative and integrated appropriately, the output from one process can provide input to the next process for the service that is delivered or supported. Processes should also be efficient, effective, and economical for the services that the process supports.

Functions and Processes

While both functions and processes enable your IT team to provide service to customers, the two are very different.

Functions are the specialized jobs performed by self-contained units that an organization sets up to achieve a specific outcome(s). An example of this is a network services team charged with engineering all, or a specialized part of, a company's network infrastructure.

Processes, as described previously, are the systems used to achieve business goals, sometimes supported with technology enablement. A process is an action or series of activities that creates change or transforms its input or trigger to move toward a specific goal and output.

Service Lifecycle

The service lifecycle is dynamic, as each stage of the lifecycle supports other stages. Specialization and coordination across the lifecycle are essential for the delivery and support of services. The service lifecycle should work as an integrated system that includes feedback mechanisms for continual improvement.

Summary

Service transition is the last stage in a project lifecycle before you go live. This place in the lifecycle is critical, because the success of the project depends on the smooth transition into service operation.

Service transition facilitates the implementation of a project that is designed to meet customer specifications and service strategy inputs. A key goal of service transition is to ensure that the expectations from the business are met. Effective service transition means the service is ready to move into operation with minimum risk, little negative impact, and knowledge management for all stakeholders.

Chapter 3
Service Transition Principles

The principles that guide service transition are derived from service strategy. The value of a given service is determined by the business customer that consumes it.

The Basics of Service Transition

With effective service transition, the business and IT can move a project smoothly from development into operation. This practice has many dimensions, both on the business and IT sides. The overarching goal of service transition is to achieve the highest level of customer satisfaction by delivering the new or improved services to the business without negatively impacting operations with outages or decreased service performance. Refer to the *Service Transition* publication for detailed lists of the purposes, goals, and objectives of service transition.

This stage in the service lifecycle adds value to the business in several ways, including the ability to simultaneously handle a heavy volume of changes and releases for multiple customers. The *Service Transition* publication outlines several additional ways in which service transition benefits the business.

How to Measure Service Transition Success

The business adage, "You must measure what you treasure," is equally true with service transition. Items that you care about need to be measured. If you don't measure your progress, you can't manage it. If you can't manage it, you can't improve it.

Following are some metrics that can help you achieve the goals of service transition:

- How many service transition plans effectively deliver the results anticipated by business units?
- What percentage of all changes to services are managed by service transition?
- What are the change success rates of projects that use service transition?
- Does adherence to service transition reduce outages and negative business impact?
- Are unauthorized changes reduced by service transition planning?
- What are the actual resources used in a deployment versus those predicted in service design?
- Are incidents, problems, and failed changes trending down?
- Are project budgets tracking with predicted values?
- What overhead does using service transition add to projects?

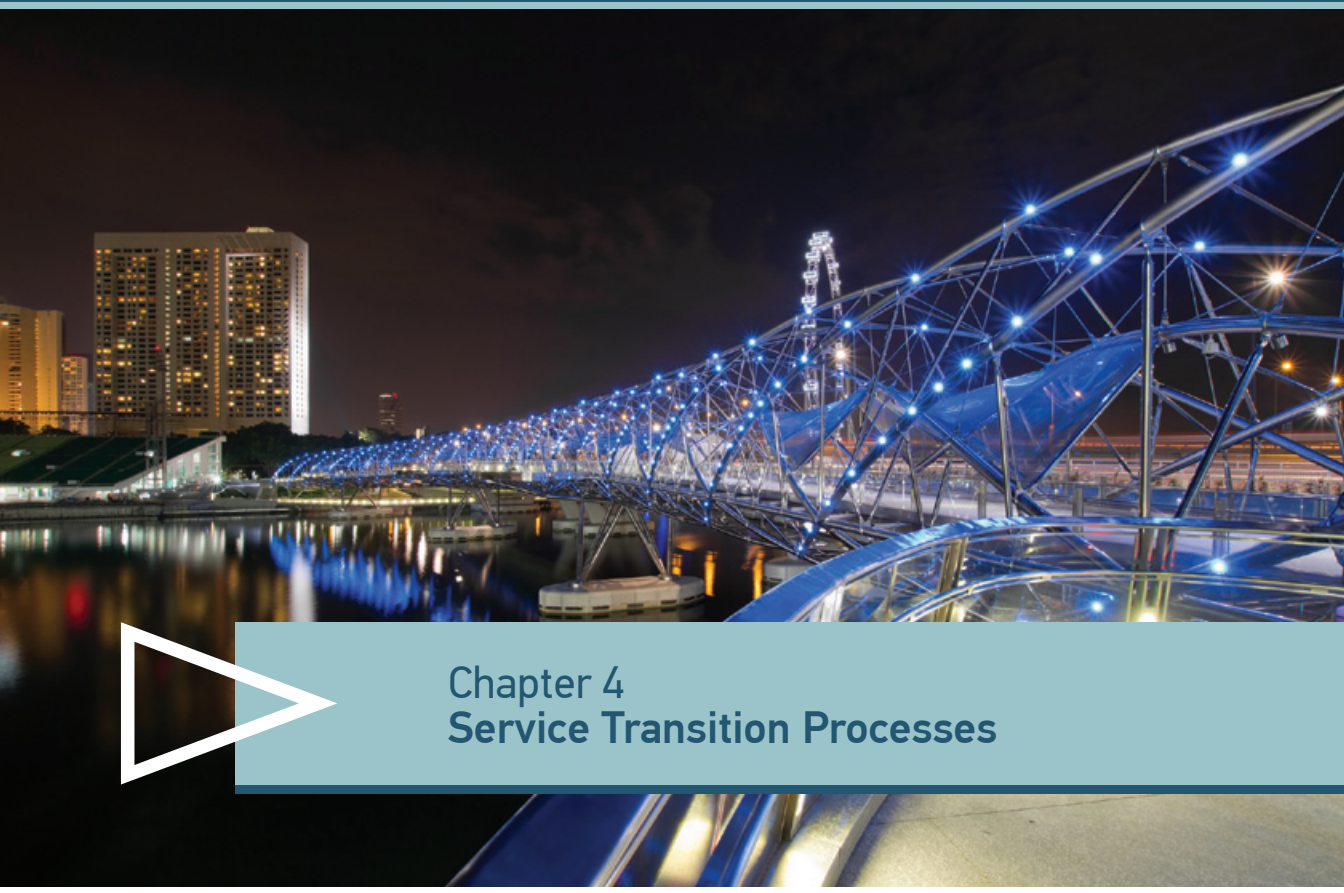
The Policy Angle

A formalized policy is necessary to ensure the success of your service transition efforts. Your IT management team should define and document the objectives and accountability for the service transition activities in your organization. This policy should fit with your existing system of controls and your overall process and governance framework.

The *Service Transition* publication describes several basic policies of service transition, along with lists of principles and best practices associated with them. These include the importance of defining and implementing a formal service transition policy, making sure that service transition is used whenever a service changes, using a common framework, providing for the transition of knowledge, correcting your course as needed, ensuring quality, and more.

Summary

Due to the changing, competitive nature of business today, the requirements for value (utility and warranty) are always increasing. You constantly need higher performance and fewer constraints so you can maintain your customers. Customers of today are no longer loyal. They may switch to the lowest-cost benefit provider or a better offer in the blink of an eye. Organizational governance, policies, and performance optimization are important principles for service value. You must be on a never-ending quest to improve both utility and warranty. Following the ITIL V3 guidance and implementing BSM will help you accomplish that goal.



Chapter 4
Service Transition Processes

This chapter represents the heart of the *Service Transition* publication. The core of service transition is encompassed in seven processes and associated activities: transition planning and support, change management, service asset and configuration management (SACM), release and deployment management (RDM), service validation and testing (SVT), change evaluation, and knowledge management. This booklet highlights each process by addressing the ITIL definition, the goal, the business benefits, and other factors to consider.

Process 1: Transition Planning and Support

A good planning team is worth its weight in gold. The maturity of the organization depends largely on how well the transition team can plan and manage all IT projects and change requests in the queue. Without planning and support, an organization will be reactive in nature, and will not grow into the kind of service and value culture that best-practice organizations enjoy today.

Definition

» *Transition planning and support* — "The process responsible for planning all service transition processes and coordinating the resources that they require. These service transition processes are change management, service asset and configuration management, release and deployment management, service validation and testing, change evaluation, and knowledge management."[6]

Goal

This process has two goals. First, through careful planning and effective coordination of resources, it ensures that you have achieved all of the requirements identified during service strategy, instituted in service design, and documented in continual service improvement. Second, it helps you pinpoint, manage, and mitigate potential risks that might disrupt service or cause it to fail during the service transition stage of the lifecycle.

Business Benefits

Service transition is primarily concerned with ensuring that the customer and the business receive the anticipated result(s) outlined in service strategy, service design, and continual service improvement, while experiencing minimum risk of service disruption or failure. An integrated approach to planning and support will help you succeed. The outcome will be your ability to handle greater numbers of changes, releases, deployments, and retirements with less work, less risk, and a higher degree of success.

Key Factors to Consider

The service design team provides service transition with inputs in a service design package. Continual service improvement provides inputs within the continual service improvement register. Other stages of the lifecycle also provide inputs; see the *Service Design* publication for a list of inputs and outputs across the service lifecycle for the various stages. Each service should have a release policy that describes details such as roles and responsibilities, exit and entry criteria, and release frequency. See the *Service Transition* publication for examples of service transition planning tools, such as a responsibility matrix and a service release policy.

Be sure to monitor the progress of a service change. Measurements recorded during service transition will enable you to create reports, track the effects of a dynamic environment, and amend your transition plans. Plan the release and deployment in stages, as the outcome of each stage has some level of uncertainty. Use proven release and deployment models to reduce risk.

The *Service Transition* publication describes the role of triggers in requests for change (RFCs) and provides lists of key performance indicators (KPIs) for the planning and support of service transition.

6 Ibid. See *Transition Planning and Support.*

Of course, each company has unique policies and will need to adapt ITIL according to its own requirements. Many organizations will need professional services or experienced people to guide them through that maze as they marry ITIL best practices with their internal needs, policies, and procedures.

Process 2: Change Management

Careful management of changes will save money and time by reducing the business's exposure to risk, lessening the impact of any service failure or disruption, and preventing failure altogether.

Definitions

» *Change* — "The addition, modification, or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items."[7]

Changes are strategic, tactical, or operational, and within these areas they can be either proactive or reactive. The intent of a proactive change is to seek benefits or value to the business or the customer, such as streamlining a service or avoiding risk. A reactive change, on the other hand, generally is made to correct an immediate situation that impacts the business or the customer in terms of service levels promised, quality of service, or quality of service experience.

A *service change* occurs when you install, remove, or modify a service and its documentation. Service changes should also be covered by change management. If a service change will have a broad impact on the organization, however, an RFC may be required. This request will enable the organization to consider the ramifications of the service change before it is made.

» *Change management* — "The process responsible for controlling the lifecycle of all changes. The primary objective of change management is to enable beneficial changes to be made, with minimum disruption to IT Services."[8]

» *Request for change (RFC)* — "A formal proposal for a change to be made. An RFC includes details of the proposed change, and may be recorded on paper or electronically. The term RFC is often misused to mean a change record, or the change itself."[9]

Goal

Change management is designed to help you avoid, exploit, or accept the associated risks when your customers' requirements demand new solutions and services from IT. This process will help you provide

7 Ibid. See *Change*.
8 Ibid. See *Change Management*.
9 Ibid. See *Request for Change*.

maximum value to your customers while reducing disruptions. It will also help in aligning your IT services with the business needs.

Business Benefits

All other lifecycle activities depend on change management to manage the risk of changes to production infrastructure; reduce the number of outages and service interruptions; increase the first-fix rate associated with problem, incident, and event management; and maintain high change success rates. The change management process also adds value to the business in several other ways, which are outlined in the *Service Transition* publication.

Key Factors to Consider

Studies from several analysts and IT think tanks show that weak change management can lead to high volumes of urgent and unplanned work. This work must be performed at the expense of important, planned work. Since outages and firefighting rarely can be put off, the demand-oriented work can often sideline projects or preventive activities. It also may lead to mistakes and oversights, causing more disruption to the business and services provided. The longer this pattern dominates, the more unreliable the IT environment becomes; it can deteriorate to the point where infrastructure availability problems literally manage IT staff.

Managing change effectively enables business continuity, operational value, and reduced risk.

IT's responsibilities are to support the business and its customers' outcomes, operate services already in production, and transition new services into production. In all of these cases, change is inevitable. Managing change effectively enables business continuity, operational value, and reduced risk.

In times of extreme system use or critical business operations, it's common for organizations to institute a change freeze. For example, many online commerce sites ban all changes from November through the end of January. For many retail businesses, the busy holiday shopping season is the worst possible time for a system failure. These merchants know that when changes are reduced, service reliability and availability are substantially increased. That's good for the bottom line.

Preventing resources from being consumed with unplanned work and firefighting is essential for optimal organizational performance in delivering and supporting projects. Changes required to transition services from development into production must be tested, approved, and scheduled to minimize risk. These steps prevent the implementation from causing its own new problems and generating unplanned work.

The interrelated nature of IT resources and specialists demonstrates the need for organizational change collaboration. Key benefits that effective change management can deliver include reduced business risk, improved scheduling, and fewer conflicts.

The bottom line is that effective change management ensures that changes being introduced into the environment go through a proper approval and post-review process to deliver new projects and reduce risk to ongoing operations.

Change Management Concepts

RDM and SACM should be tightly coupled with change management. Some immediate benefits of their integration center around the better balancing of release and change activities with the need to manage configurations and understand the potential impact of proposed activities before they begin.

During change management, each change has associated tasks that happen either sequentially or in parallel. The tasks include risk and impact analysis, planning, and approval prior to implementation. Such activities should be supported by an established workflow. A critical success factor for a complete risk assessment and impact analysis is an accurate and reliable configuration management system (CMS). This booklet discusses the CMS later in this chapter and in Chapter 7.

When designing or updating your change management policy, be sure to delineate the different types of change requests and their criteria. This clarification can eliminate the need to invoke entire activities within the process when you only need to perform a post-evaluation to assess if the change is still a low-risk change and can remain as a standard or preauthorized change. Do not treat each change as though it presents equal risk to your operation; this approach can constrain your change management process with regard to the business value that can be achieved. There are three common types of RFCs:

- *Standard changes* are often preauthorized. They represent low-risk, common activities with a known outcome. (These can be services that are entered into the service catalog. Then the user community can select from the request fulfillment service to order such things as cloud services, new users, modifications to applications, access rights, etc. Standard changes can also be routine IT changes that are considered low impact. The change management process activity of post-implementation review should be performed in case the change has been associated with, for example, an increase in incidents or a high-impact outage to particular services.)
- *Normal changes* should follow the change management process from the beginning of the process and should include all activities. The impact of these changes to the business can be significant until determined that they are low impact. If the changes are low impact or nonsignificant, the standard change procedures can be followed. Changes get prioritized, authorized, and scheduled. Then change management coordinates the change implementation while release and deployment executes the change.

» *Emergency changes* follow the same flow as a normal change, but on an accelerated timescale. Usually, testing and documentation are minimized so that adequate personnel are available to accommodate the release and rollout, thereby compensating for the high risk involved. Following the implementation of an emergency change, however, the full documentation and — if necessary — future testing should occur to ensure stability of the implemented change.

It is not best practice to approve a change request for a high-impact emergency change that does not contain a detailed back-out or remediation plan in the event of failure. Be sure to describe how the affected service or infrastructure will be restored to its original state if the change fails and must be aborted.

While some changes truly cannot be undone, the goal of change management is to reduce such activity to a bare minimum. If the proposed change will be irreversible, then it must be fully tested to ensure it will work as planned. If the change doesn't succeed, you may need to completely rebuild systems from a previously established configuration baseline, or invoke a business continuity plan to recover from the damage.

Careful Planning for Improved Success

To effectively and consistently evaluate proposed changes, develop a standardized impact risk assessment form on which change assessors can objectively evaluate each request. Consider the potential of the proposed RFC to disrupt services, as well as the consequences of change failures. The assessment can be modified over time to reflect lessons learned and unique business constraints.

See the *Service Transition* publication for lists of the primary tasks for managing general change activities or individual changes. These include activities such as planning for, scheduling, communicating, and authorizing changes; creating remediation plans; measuring, controlling, and reporting changes; change impact management; and continual improvement.

Consider the potential of the proposed RFC to disrupt services, as well as the consequences of change failures.

When delaying a change puts the business at risk, carefully analyze the risk, then present the change to the business for signoff, disapproval, or rescheduling. The business risk will weigh more heavily as a deciding factor when considering whether the risk of IT failure is worth taking. It may be wise to document that you have carefully evaluated the risk before proceeding with the change. Timing may be critical, too. In some cases, owners of business services may be content to continue with the problem to meet their own objectives and goals (such as end-of-quarter sales), and wait until after that period to make the change.

Preventing risky activity is one benefit of change management, but the power of planned work through effective scheduling is equally important. In many organizations, several critical resources are required for any substantive change. By combining like activities and grouping discrete changes into broader release packages, you can more efficiently deploy critical resources.

The schedule of changes (SC) contains all pertinent details regarding approved and scheduled changes. Establishing dedicated maintenance windows will improve change success rates and increase operational efficiency. You can then package multiple changes into a single release and test all changes together as a single unit of release. These windows must be established in accordance with the needs of the business. Typically, these windows are scheduled outside of peak business activity and are large enough to accommodate regular maintenance activities without causing business disruption — or to accommodate rollback, if necessary.

In addition to reviewing proposed changes, the CAB must also review changes that already have been implemented.

An essential component in every proposed change is the projected service outage (PSO) time, which estimates the time it will take IT to complete the change-related activity and restore service to affected business customers. The SC and PSO are primary elements of approved changes that must be derived in concert with business stakeholders so there is ample time to plan alternate activities or other ways for business staff to stay productive. They are also major determinates of scheduling and resource planning.

Put Your Trust in the CAB

The role of the change advisory board (CAB) is the evaluation and oversight of proposed changes, as well as evaluating the categories of proposed changes that are not defined as standard — both before and after approval. In addition, the CAB validates that these potentially higher-impact changes are tested and properly documented wherever possible. It also has the responsibility of "signing off" on standard changes that are added to or modified in the service catalog.

Include in the CAB meetings the key stakeholders who have responsibility or accountability for the service or the stakeholders who need to be consulted, such as the service owner, representatives from the business areas impacted, problem management, incident management, and/or service asset and configuration management. Stay focused on the needs and impact of the proposed activity on your customers and users.

In addition to reviewing proposed changes, the CAB must also review changes that already have been implemented. The lessons learned and the resulting recalibrations can be well worth the effort. The CAB also helps improve the change management process itself.

There are several reasons for reviewing *all* changes after they have been implemented. A review will tell you whether the change actually met its desired outcome and objectives, and whether all stakeholders are satisfied with the end results. You'll be able to identify any unexpected conditions (performance side effects, functionality issues, etc.) and to determine whether the change required more or fewer resources than planned. A change review will also verify whether the change met budget targets and was implemented during the proposed PSO window. You can also ascertain the success of rollback, in the case of change failure.

ECAB to the Rescue

When there's not enough time to convene a full CAB meeting, or the lateness of the hour prohibits it, the emergency change advisory board (ECAB) comes to the rescue. This smaller group of CAB members must have the authority to make decisions in case of emergency. Carefully create a policy and outline the procedures required to invoke the ECAB and what steps are involved once it convenes. The ECAB is charged with representing business and technical perspectives in order to make the best change decisions, no matter what the situation. It should not be used to circumvent the normal CAB meetings and must be used only in an emergency situation.

An astronaut is not going to let go of the controls to complete a report while stabilizing a crippled spaceship. In the middle of an emergency, you won't have time to do all the paperwork that ITIL requires, either. The documentation can wait until you have the situation under control. When you implement an emergency change, most likely you won't be able to test it very thoroughly, so you'll need more people to help out. You can come back afterward to retrofit the actual change process and release documentation, then update your SACM later.

Change Management KPIs

Metrics are essential before, during, and after a change. Metrics help you understand causes, effects, trends, and the speed of the IT response. Metrics provide factual data for decisions.

When using metrics, be sure to understand the goal of any process or function. If you understand the goal, you can decide what outcome you want to create. From the outcome, you can derive the key performance indicators (KPIs). Each process and function should show an improvement toward the overall goal of that process and the service that is supported by the process.

Refer to the *Service Transition* publication for a list of KPIs for change management, along with examples of common metrics used to measure change.

Process 3: Service Asset and Configuration Management

The effective use of business assets to deliver a quantifiable return is one of the classic attributes of a successful manager. This concept extends into the management of IT service assets as well, and articulates the underlying value of service asset and configuration management. Although service asset and configuration

management are closely associated, there are different consumers of the data from an asset perspective versus a configuration management perspective. The knowledge management process can help distinguish the data needed for various stakeholder decisions. Organizations may want to have one person or function accountable but have separate coordinated responsibilities for asset and configuration management.

Definition

» *Service asset and configuration management (SACM)* — "The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets."[10]

Business Benefits

SACM manages all of the service assets from cradle to grave and is a key player in supporting all service management processes, including change, incident, and release management.

The savings inherent in the proper management of assets, software licenses, and configurations can be massive.

The savings inherent in the proper management of assets, software licenses, and configurations can be massive. The SACM processes and knowledge output are crucial to the effective management of changes, releases, service level agreements, warranties, compliance, and cost controls.

Key Factors to Consider

SACM is used to protect the integrity of configuration items (CIs), as well as the service assets they contain, through the entire service lifecycle. It actively monitors, controls, and reports on the status of the CI and service configurations under management. It uses a comprehensive CMS to monitor, manage, and control configurations. And, it provides up-to-date and accurate information and status regarding assets to other processes (such as change management) and other departments (such as finance).

The ITIL definition of a *configuration item* includes "any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements."[11]

10 Ibid. See *Service Asset and Configuration Management.*
11 Ibid. See *Configuration Item.*

ITIL defines a *service asset* as "any capability or resource of a service provider."[12] ITIL's definition of an *asset* includes "any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure or financial capital."[13]

SACM must create a logical model of the IT infrastructure. This model, or map, details the dependencies and relationships between the CIs and service assets. The model is also crucial for other process areas, such as change management, where the relationships between CIs can illuminate potential risks and service impacts. In problem management, SACM can point the way from a failed CI to the services it impacts.

For SACM to deliver this valuable contextual information, it is imperative that the records kept in the CMS are as accurate as possible. The data is used for decision support across the service lifecycle. By building accurate, logical maps of CIs that flow upward to the services they underpin, it is also possible to save time and effort on compliance-related activities.

Compliance with legislation, such as the Sarbanes-Oxley Act of 2002, requires that the CEO and CFO of public corporations attest to an effective system of internal controls over financial reporting. Most modern business financials are derived from IT systems, especially enterprise resource planning (ERP) and customer relationship management (CRM) systems.

An organization that has effective SACM can generate a list of all CIs and service assets that support financial reporting. Once the assets are identified, a system of controls can be built to guard their unique integrity requirements and establish configuration baselines with which to demonstrate their operational integrity. This will include reporting and managing changes to the critical financial systems and services.

Managing CIs and Service Assets

SACM is not only responsible for managing CIs and service assets from their inception to their retirement. It must also manage their configurations. Asset management is accomplished in various ways, depending on the type of assets.

For *infrastructure assets*, baseline the software and configurations, and then have them automatically audited against the baseline. This alerts SACM and change management when an unauthorized or inadvertent change is made to the asset. In that event, SACM works with the respective process area to bring the issue to resolution (either rollback or approval of the change) and then update the CMS to reflect the new state.

12 Ibid. See *Service Asset*.
13 Ibid. See *Asset*.

Some organizations find that only certain types of infrastructure should be under the SACM umbrella. Lower-cost and less-critical infrastructure may not be included, such as desktops or mobile devices. In other organizations, a great deal of money can be made or lost at the desktop level (by stock traders and analysts, for example). And still other, larger companies may want to manage only mission-critical, shared-service delivery infrastructure under SACM. Start with an understanding of the business needs and drivers in your company, and then reflect those needs in your initial SACM policy.

You can protect *service assets* with some form of content revision control. These assets require many levels of documentation and agreements that define the services. SACM is responsible for keeping pointers to the original documents and verifying that they are in their last-known state.

Register *media assets*, such as installation disks, backups, disk images, release packages, and golden-build specifications, in a definitive media library (DML). Revision control is a must for media assets, since there likely will be more than one version of a particular application in use at any given time. A variety of content and revision control software titles are available to accomplish this task.

Get a global view of all assets that could potentially be affected by an outage or service interruption.

SACM is also responsible for managing the entire lifecycle of the assets — and associated costs — from their purchase, installation, and use, to retirement. Establishing a controlled environment in which the desired run state of every CI is both known and protected is critical to reliable operations. Not only does effective SACM contribute to reliability, but it also enhances predictability for new or modified services that are launched into production. By ensuring production configuration consistency, it is now possible to bring the exact production configurations into the test environment. This ensures accurate and consistent quality assurance activities.

Take a Global View

SACM hinges on an accurate relational model of assets, services, and infrastructure. The logical model created by SACM is essential to other processes that depend on understanding the complicated and ever-changing relationships between IT assets. This information is crucial to problem and incident management, change and release management, and planning operations; it will help reduce the risk of protracted outages and service interruptions.

Before taking any action, and before you find yourself fighting fires, get a global view of all assets that could potentially be affected by an outage or service interruption. To use your IT infrastructure to its fullest capability,

combine this contextual model with external data to optimize usage and to reduce costs. A prime example would be understanding actual software license usage versus projected budgets. Are you using more or fewer licenses than projected? Are you out of compliance and at risk of being fined?

The Configuration Management System

Storing the data in model form for all of the CIs under management, as well as their contextual relationships, requires the use of a configuration management database (CMDB). However, the CMDB needs to be fed by auto-collection tools, and it requires federation to source data. It also needs to be analyzed and the findings presented. This procedure helps you create a configuration management system (CMS).

A CMS can be used by a wide range of business processes. For example, a CI could be a maintenance contract with a third-party supplier. It would contain the actual contract as an attachment, as well as information about the supplier, the organization, the contract signing and expiration dates, and any related service level agreements (SLAs). The same record could also contain a relationship to a service that is underpinned by the contract.

Some organizations may need multiple federated CMDBs. In this case, the detailed CIs that describe staff, service, and system owners, as well as supplier and vendor data, come in very handy. Imagine trying to figure out why a service is down, only to find that the faulty CI is located in another hemisphere and maintained by a third-party vendor.

With a CMS, you have related normalized data that can give you contact information, associated incident or problem records, a view of all work and configuration changes performed, and a detailed list of the services and SLAs from the provider. Chapter 7 of this booklet discusses the CMS and CMDB in greater detail.

Security Counts

Within SACM, a *secure store* is a place where IT assets are located. A secure store comes into play when the asset needs to be in a known working state, such as a service spare or replacement parts. The secure store is a major component in a successful service continuity or restoration program.

Another critical security measure is to place master software libraries, file storage, copies of all developed and controlled software, and master copies of system documentation in the DML, as mentioned earlier. The CMS and DML both contain a variety of critical information. Develop a backup and restore policy for this data.

Choosing the Right Level of CIs

Start planning a CI's identification with a single, critical business service; don't try to deal with the entire catalog at the outset. Using a top-down, straw-man approach with a service will show you just how much detail you really need to achieve benefit.

The primary value of the CMS is the relational dependency model it creates. Focus on capturing the relationships to shared and common infrastructure, such as incidents, problems, changes, and SLAs. Also focus on gathering the versioning and configuration baseline data necessary to traverse and monitor known configuration states with a high level of confidence.

Establish naming conventions from the beginning for consistency and to alleviate confusion. For quick identification, consider bar coding the CIs or use radio-frequency identification (RFID), or something similar.

The Importance of Audits

Developing an audit approach to managing the CMS and its contents should be based on the risks. If your company is regulated, there may be serious drivers to maintain configuration management integrity that reach far beyond the normal management concerns present in many companies. If your organization is audited by an internal or external audit group, these activities may constitute part of a control self-assessment. Either way, talk with your IT auditors to understand their auditing criteria and guidelines (e.g., COBIT).

You can take several actions to reduce the risk of failed changes or unexpected implementation results:

- Routinely audit the variance between the configuration baselines contained in the CMS and the actual, deployed production environment.
- Physically verify the existence of CIs in their native environment (the data center of the DML).
- Perform an extra verification of the supplied documentation before allowing a release to proceed.
- Audit after a release to make sure the CI's actual configuration conforms to the expected baseline.
- Audit via discovery tools to find any CIs that are not in the CMS.

If you notice a significant level of variance in any audits, develop a remediation plan and increase the frequency of the audits until the situations driving the variance have been addressed. BSM technology can help you achieve high performance in this area.

Process 4: Release and Deployment Management

The scope of release and deployment management (RDM) includes the various systems, processes, and functional roles required to build, effectively test, plan, and ultimately deploy a release in order to establish a service into the production environment.

Definition

- *Release and deployment management* — "The process responsible for planning, scheduling and controlling the build, test and deployment of releases, and for delivering new functionality required by the business while protecting the integrity of existing services."[14]

14 Ibid. See *Release and Deployment Management.*

Goal

The overarching goal for RDM is to build, test, and provide the capability and resources to deliver the services conceived by service design or continual service improvement, which are based on business stakeholder requirements.

Business Benefits

Through effective RDM, IT can provide immense business value by shifting resources to the lifecycle point at which the cost of defect repair is lowest. Just as in manufacturing, the cost of defect repair multiplies as the product moves down the assembly line, and increases considerably when the item leaves the factory. By developing a rational approach to managing software and configuration releases and their subsequent deployments, the cost of outages, rework, and unplanned work can be reduced dramatically.

RDM benefits the business by ensuring that changes are turned around faster due to less rework and firefighting. This process is very significant as it relates to agile provisioning for cloud computing services. RDM makes certain that services delivered actually meet business needs and goals. It provides a consistent approach to repetitive and low-risk work, such as rolling out changes. And it creates a consistent, verifiable, and fully auditable approach.

Through effective RDM, IT can provide immense business value by shifting resources to the lifecycle point at which the cost of defect repair is lowest.

Key Factors to Consider

Release units should be defined by policy that governs and provides guidance as to what kind of releases can take place and what their cycle is. ITIL defines a *release unit* as "components of an IT Service that are normally released together. A release unit typically includes sufficient components to perform a useful function. For example, one release unit could be a desktop PC, including hardware, software, licenses, documentation, etc. A different release unit may be the complete payroll application, including IT operations procedures and user training."[15] A release unit can be based on a cloud provisioning blueprint.

Considerations for release and deployment can be described by two differing approaches. The big bang approach focuses on delivering releases to production all at once. The phased approach plans the delivery rollout in carefully controlled waves. Releases can also use the push/pull approach. See the *Service Transition* publication for a discussion of the many variations and options based on these approaches.

15 Ibid. See *Release Unit*.

Establishing release windows is also paramount to the ability to successfully determine how many releases and of what type can be scheduled during a given period. Coordinate with the SACM and change management processes to determine an overall time window that avoids collisions.

> The validation step is the last chance for ensuring that the new or modified services meet strategy and design requirements and that the expected benefits will be achieved.

See the *Service Transition* publication for specific activities around release and deployment guidelines, their respective pass and fail criteria, and how to build and test releases prior to their deployment to production. The publication provides highly detailed and practical, tactical guidance for building an RDM program.

Early Life Support

Early life support (ELS) details the activities and controls necessary to transition a new or modified service into service operation in a controlled manner. Transition and operations work together for a defined period after implementation.

The ITIL definition of *early life support* is "a stage in the service lifecycle that occurs at the end of deployment and before the service is fully accepted into operation. During early life support, the service provider reviews key performance indicators, service levels and monitoring thresholds and may implement improvements to ensure that service targets can be met. The service provider may also provide additional resources for incident and problem management during this time."[16]

The ELS plan specifies the activities and is defined in the service design stage. ELS outlines which resources are necessary to resolve operation support issues in the shortest time. The ELS plan operates for a defined amount of time and contains specific exit criteria based on the overall performance of the new or modified service.

Key Metrics

The KPIs for release management include measuring the variance between service requirements and actual performance; a reduced number of incidents caused by the new or modified service; an improvement in user satisfaction trends; a reduction in unplanned work associated with a new or modified service; and a reduced level of variance between the planned end state and the actual end state of CIs.

16 Ibid. See *Early Life Support*.

Process 5: Service Validation and Testing

ITIL provides comprehensive guidance on service validation and testing (SVT), including levels of testing and various test models. SVT is concerned with reducing the lifecycle costs of services and release packages by catching defects, incorrect assumptions, and missed design elements before they hit the production environment.

The validation step is the last chance for ensuring that the new or modified services meet strategy and design requirements and that the expected benefits will be achieved. The testing step is critical yet often neglected because of time and budget constraints — frequently at the expense of other services and, ultimately, at the expense of the business. This adds far greater cost and time delays. Proper testing will help ensure that an implementation or change is successful. Remember, the objective of service transition is to ensure little or no disruption to the business while making additions or changes that are important to the business. Validation and testing is the final "catch-all" step; it must be used.

The applications team will be eager to get the new service into production, but operations will want to ensure that the system has been appropriately tested. Remember, it costs less to fix problems now than it will cost later. Once the service is in production, the service operation team will most likely be held accountable for any failures, regardless of the cause.

Services that are properly validated and tested are reliable.

Definition

» *Service validation and testing (SVT)* — "The process responsible for validation and testing of a new or changed IT service. Service validation and testing ensures that the IT service matches its design specification and will meet the needs of the business."[17]

Goal

SVT aims to provide quality assurance (QA). This is accomplished by validating that the service provided is indeed fit for its purpose and will be usable by its customers. SVT also includes testing that the service or release actually functions reliably.

Business Benefits

Services that are properly validated and tested are reliable. They also provide the business value and remove constraints as conceived during the service strategy and design stages.

17 Ibid. See *Service Validation and Testing.*

Key Factors to Consider

KPIs for SVT include reductions in all of the following: effort and cost to build the test environment, unplanned work associated with SVT, incident- and problem-related activities associated with SVT, the overall balance of errors across the whole lifecycle, and the number of known errors documented in earlier testing phases. The KPIs will aid the continual service improvement process, too.

You've invested a lot of time and resources in developing a strategy and designing how you will provide the service. Don't transition it into production without putting it through a rigorous test process.

Process 6: Change Evaluation

Change evaluation may be the most intuitive of all ITIL processes. It is concerned with understanding whether the performance value of a proposed activity is acceptable and whether it ultimately will provide enough return to guarantee budget (or prove return on investment [ROI]) and subsequent adoption.

Definition

» *Change evaluation* — "The process responsible for formal assessment of a new or changed IT service to ensure that risks have been managed and to help determine whether to authorize the change."[18]

Goal

The goal of change evaluation in the service transition process is limited to evaluating the actual versus the predicted performance of any service change. By looking at the expectations that were set prior to the change, you can determine the following: *Were the expectations met? Was the performance in line with expectations? What lessons can be learned for the next change or release?* Change evaluation is also where the return on value can be assessed to ensure that the value the business specified in the service strategy is being met.

Business Benefits

At the very heart of this process is the protection of business value. The more effective the evaluations of change and service implementations are, the better those activities ultimately serve the business. The data gleaned from this process can then be translated into goals for continual service improvement efforts. The value can be both in the present, by rectifying situations where the delivered value is not in line with the expected value, and in the future, by improving the activities and processes that produce the new service or release.

Key Factors to Consider

The *Service Transition* publication outlines a policy to support change evaluation. The first step is to evaluate service designs and changes before they are deployed into production. Second, get the customer or primary

18 Ibid. See *Change Evaluation*.

stakeholder to sign off any variance between actual and expected performance; otherwise, reject the change, roll back, and start again with a new change. Third, complete a customer engagement package to document acceptance signoffs or rejection intent. The process inputs for evaluation come from service strategy, design, continual service improvement, and SACM documentation. The primary outputs of this process are the evaluation reports that flow to change management.

Process 7: Knowledge Management

An IT organization's ability to deliver on its promises to the business depends on its knowledge of how to act and respond in a variety of situations. The ability to understand the situation at hand, and to evaluate the options and risks, plays heavily into the ability to be successful at multiple levels. This includes the tribal knowledge within individuals' heads.

Definition

» *Knowledge management (KM)* — "The process responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time. The knowledge management process enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge. *See also* Data-to-Information-to-Knowledge-to-Wisdom; service knowledge management system."[19]

Goal

The overall goal of KM is to improve both the quality and the availability of critical data to enable accurate management decisions that serve the business. ITIL defines the scope of KM as the entire service lifecycle.

Business Benefits

Knowledge management provides value to the business in several ways. It enables better service quality through increased IT efficiency and increases the understanding among IT staff of the value of services provided to the business. It ensures that the IT staff always knows who is depending on its services, how much they are consuming, any particular service-related constraints, and any shortcomings or issues the customers are currently experiencing with the services. Knowledge management keeps your company's intellectual property separate from that of competitors and outside service providers. To ensure effective transition from design to operation, critical knowledge and lessons learned from past implementations must be readily available. Passing information to stakeholders to make a *go* or *no go* decision is a major benefit of knowledge management. Knowledge management should influence how data is collected and transformed to information and then how information is transformed to knowledge for stakeholder decision support.

19 Ibid. See *Knowledge Management.*

Key Factors to Consider

Data-to-information-to-knowledge-to-wisdom (DIKW) is defined by ITIL as "a way of understanding the relationships between data, information, knowledge, and wisdom... [that] shows how each of these builds on the others."[20] DIKW provides a structure that describes how data can become useful. Data that is not useful should not be collected and managed by IT.

The entire organization benefits from knowledge management and the ability to make collaborative decisions.

ITIL defines a *service knowledge management system* (SKMS) as "a set of tools and databases that is used to manage knowledge, information and data. The service knowledge management system includes the configuration management system, as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analysing and presenting all the knowledge, information and data that an IT service provider will need to manage the full lifecycle of IT services."[21]

Challenges in KM include deciding what to capture and how to maintain it, transferring the knowledge, and measuring the value.

The entire organization benefits from knowledge management and the ability to make collaborative decisions. The ability to resolve issues quickly by having the information at hand reduces lost time due to employees not knowing what to do and results in a reduction in mean time to restore service (MTRS). In addition, incidents that can be tied to a new or changed service can be fixed or averted through information contained in the knowledge base.

In building an effective knowledge management system, keep in mind that people like to protect their knowledge, especially when there are rewards and recognition for doing so. The ultimate goal is to foster a secure environment in which people are rewarded for sharing. With a free flow of knowledge and wisdom, people grow, the organization grows, and management is able to make the wisest decisions possible. Knowing both the skills and people resources will enable you to put together the appropriate teams for project work, change evaluations, and so on.

Summary

By understanding the seven processes associated with service transition, you will be able to more effectively move your services into operation. All the process areas are important. If you use one without the other, you will have gaps in your capability to deliver and support high-performing services to your customers.

20 Ibid. See *Data-to-Information-to-Knowledge-to-Wisdom.*
21 Ibid. See *Service Knowledge Management System.*

Chapter 5
Managing People Through Service Transitions

Two essential service transition activities are managing communication and managing organizational and stakeholder change. The *Service Transition* publication places strong emphasis on garnering early business support for the proposed transition. This is where service transition must embody organizational change and development tactics that work well in your particular corporate culture.

Organizational Change Management

When IT is rolling out a new service, it's not enough to roll out a new technology without any processes in place. If so, the technology is useless and you will not create value for the business. Likewise, if you have the best technology in place and the best processes defined, but the people aren't trained to run the new service, then you also will not realize full value. As most CIOs will tell you, you want an equal balance among the enabling technology, the processes, and the people to get the full value potential back to the business. You must also educate people on the business value of a new system and train them in its use.

Be sure you have a solution adoption strategy. Maturity assessments, gap analyses, and business simulations provide an opportunity for IT organizations to view the benefits that they can gain by adopting new

processes. When people can experience the new possibilities through simulations, they're more likely to buy into the idea and get excited about it. Often, it then becomes easier to achieve the necessary organizational development and to move to the next level of maturity.

You want an equal balance among the enabling technology, the processes, and the people to get the full value potential back to the business.

Adjusting to Change

Address the emotional cycle of change; without the support of the people involved, there will be no change. To minimize the time required to accept changes, establish the role of service transition as providing the following: leadership that embraces the change; planning that supports adoption by the organization; the development of capabilities needed for the change to take place; metrics that you can use to manage the process; and an inclusive, "everyone's opinion counts" style of feedback management. Create a sense of urgency in your organization. Communication is key to success; let people know about training, installations, and success. Celebrate success!

Summary

While the efforts to manage service transition fall under many process and activity areas, the broad approach to managing organizational change must evolve to include the needs and voices of business stakeholders. By including these valuable voices throughout the lifecycle, changes will ultimately deliver more of the promised value to the business. Be sure, too, to balance IT stability with the business need for change. Be careful to manage your projects so that you achieve quick wins. To evaluate project success, use factual KPIs and data, as well as expert opinions from your stakeholders.

Run book automation solutions enable you to streamline IT operations by automating routine, labor-intensive, error-prone tasks and by leveraging systems, applications, and tools across silos — from trouble ticketing to fault management to performance monitoring to virtualization management to the CMDB. They also help you automate release and deployment tasks. Managing across silos is a key focus of ITIL. As such, a comprehensive run book automation solution should provide out-of-the-box, ITIL-based process workflow to help you automate these manual, repetitive processes.

By uniting management systems and technologies with best-practice ITIL processes, run book automation delivers a unified service delivery capability.

By uniting management systems and technologies with best-practice ITIL processes, run book automation delivers a unified service delivery capability. Run book automation not only overcomes the barriers of technology, process, and organization (people), but also unifies the parts to work together efficiently and provide dependable service delivery. Once the links are established among technology, process, and organization, you can then begin to view the services you deliver to the business as just that — services — rather than focusing on the individual components. When you start looking at the services as a whole, you gain a better understanding of the end-user perspective. For example, the end user really only cares that the service is available and working as expected, and that's what IT needs to measure. If the sales order application isn't functioning, it doesn't matter if all the individual infrastructure components supporting it appear to be working properly. To the end user, IT has failed. ITIL provides a framework for adopting a service lifecycle approach and proper business perspective. IT then needs to establish service levels in accordance with business priorities to most effectively allocate resources (both people and technical resources) to the areas that matter most.

Run book automation solutions provide monitoring and measuring capabilities so that you know how the automation is affecting the overall process. This also enables you to adopt a continual service improvement program, another cornerstone of ITIL.
— excerpt from "Run Book Automation Sets the Stage for Business Service Management," *VIEWPOINT, Focus on: Service Automation*, published by BMC Software, 2007

For a more thorough list of systems that support service transition management, refer to Chapter 7 of the *Service Transition* publication.

The Importance of a Configuration Management System

A variety of additional tools are available to support effective service transition. The following ITIL definitions are key to this discussion: *configuration item (CI)*, *configuration management database (CMDB)*, *configuration management system (CMS)*, and *service knowledge management system (SKMS)*.

Chapter 6
Organizing for Service Transition

The service asset and configuration management (SACM) process presents some classic organizational challenges in that its activities are not confined to a departmental silo but are, instead, spread among various departments across the entire IT organization. It is crucial that the activities also be mapped into these discrete departments or units as organizational responsibilities. This approach allows the managers of the departments to have SACM at the heart of their immediate operating principles and goals.

One person or function should always be accountable for each service, process, and function within ITIL. This ensures that someone is always watching after the maximum efficiency, effectiveness, and coordination of all responsibilities, information, and consultation required for the whole of IT to operate as one.

Communication During Service Transition

Expectation setting is an important aspect of service transition. The business will develop requirements and set a timeline for their completion. It's the role of the service transition team to communicate with the business and appropriately set expectations. It may turn out that IT will not be able to deliver all of the requirements within the time frame desired by the business. Therefore, the business may be asked to prioritize the critical

To understand the full value of a CMS, first consider the role and importance of a CMDB. A CMDB is a repository of information that relates to all the components, or CIs, associated across the IT environment.

Providers of IT management solutions offer commercial CMDBs to hold configuration data and make that information accessible to the management applications that need it — whether the application is a data provider or a data consumer. The CMDB provides a single point of reference, making it the definitive reference mechanism for all IT decisions. It provides business-aware visibility into the dependencies among business processes, users, applications, and underlying IT infrastructure.

The leading CMDB solutions are built to support a federated CMDB approach, meaning that not all configuration data must reside in a single physical database. The concept of federation relies on the premise that the CMDB should contain only needed data, while still being able to do its job. Other data sources and systems can be related to or federated to the CMDB without putting all the information within the CMDB itself. In fact, ITIL now recognizes the importance of this federated approach and recommends that it be a core part of the structure of a CMS.

The CMDB provides a single point of reference, making it the definitive reference mechanism for all IT decisions.

With federation, core data is stored in the CMDB, just as information about a person or a business can be stored in a telephone directory. Then, all detailed and related CI data are federated, which simply means that a centralized database is linked to other, more detailed data stores. This linkage provides a CMDB access to the entire library content (the CIs). Hence, the CMS includes the CMDB or multiple CMDBs and, through federation, provides access to all primary data stores and their respective contents, thus providing a normalized single source of truth for organizational business decisions.

The core function of the SKMS is to help IT organizations solve problems or make decisions from the collaborative business perspective. By ensuring all IT management applications have access to properly cataloged IT configuration data, the SKMS can provide you with the insight necessary to make improved business decisions. This approach is known as Business Service Management (BSM), another best practice featured in ITIL. BSM solutions, when deployed effectively, dynamically guide IT actions and decisions according to their impact on business services. They should provide out-of-the-box support for best-practice IT processes, automated technology management, and a shared view of how IT supports business priorities.

Eliminating Manual Effort Through Auto-Discovery

Although the *Service Transition* publication does not provide details on discovery, here are some things to think about.

elements that need to be accomplished within the time frame and select any requirements that can be pushed out to the next phase.

An effective service transition continuum includes *all* relevant stakeholders — not just IT staff — in the processes of scheduling and resourcing. During testing, validation, and deployment, there are many essential communication and touch points. Be sure to engage the business early in the project's lifecycle to alleviate potential problems.

The biggest value of the RACI model is that it clearly describes the roles that people should play in service transition.

Defining Roles

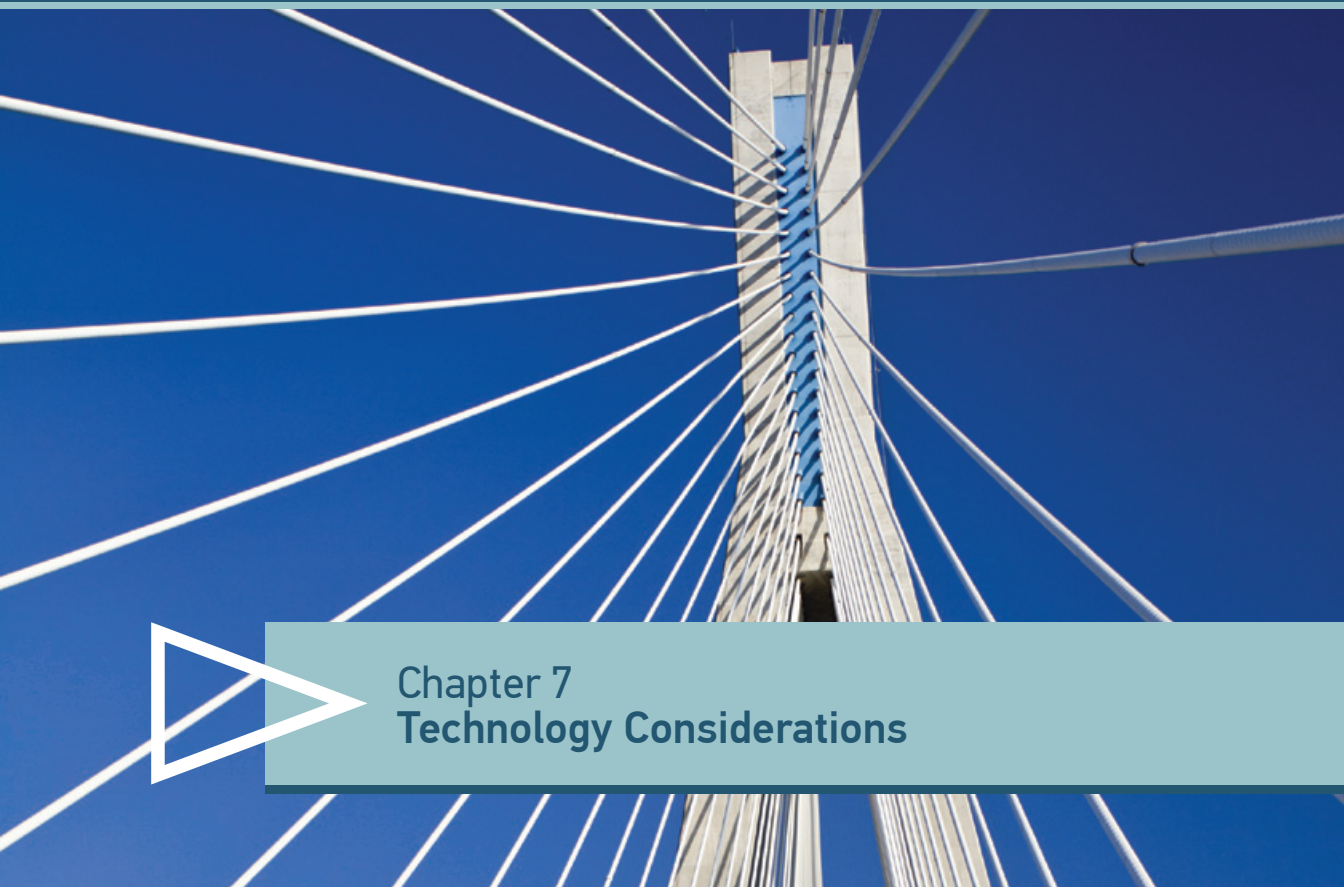
The *Service Transition* publication describes generic and specific roles needed during the transition stage. Different people may take on portions of the RACI model (responsible, accountable, consulted, and informed) of these roles, depending on the process.

The biggest value of the RACI model is that it clearly describes the roles that people should play in service transition. It identifies who is accountable for particular areas, who needs to be informed of activities, and who should take specific actions. This comprehensive list of roles and responsibilities helps eliminate confusion and ambiguity. When people fully understand their roles, collaboration improves and there will likely be fewer bottlenecks to delay decision making. The model provides an activity analysis to help identify whether more than one role is accountable for an activity, or whether too many people are involved. It's appropriate to share responsibilities as long as the roles are clearly defined.

Several roles are critical for successful service transition. The transition management team is responsible for participation in the full ITIL lifecycle. It works with the business strategy teams, as well as with the design and operations teams, to ensure that a new or improved service meets their collective requirements.

Summary

Keep in mind these success factors: A single person or function is accountable for every process, service, or function. The process, service, or function owner for service transition works closely with the other lifecycle teams. For example, when rolling out a new service, the transition team helps set expectations and should be involved at the beginning of the design stage. The transition team also helps with unit and integration testing. In the service operation stage, the transition team evaluates whether the rollout actually meets the original requirements. Please refer to the Skills Framework for the Information Age (SFIA), which is a common reference model for the identification of skills needed for IT services.



Chapter 7
Technology Considerations

Technology supports the service transition process in two important ways. It supports tools that affect the entire service lifecycle. And, it supports the service transition part of the lifecycle and smaller elements within service transition.

Chapter 7 of the *Service Transition* publication talks about two main categories of systems that provide support for the broader scope of *service transition management*. The first is *IT service management systems*, which allow the following activities: managing systems, networks, and applications; providing managers with visibility through dashboards and reporting tools; and linking in the CMDB or other tools through an enterprise framework.

Enterprise-Wide Tools

The first main category of systems supporting service management is tools that affect the entire lifecycle. Examples of this are an integrated IT service management system and dashboards.

The Importance of a Comprehensive IT Service Management System

To meet business demand for dependable, technology-driven services, IT organizations need integrated service management processes that consider technology components as interrelated parts of services IT provides to the business.

Look for an IT service management solution that integrates the service desk application with incident, problem, change, asset lifecycle, and service level management applications, and that removes silos of disciplines and services. An effective service management suite will also have a CMDB, workflow platform, and user interface, thereby integrating and automating processes across the solution, as opposed to field-to-field integrations. This unified approach provides proactive and continual improvement of service availability, quality, and cost-effectiveness in complex enterprise environments.

Dashboards Provide Visibility into IT Performance

A dashboard solution provides highly interactive, right-time access to service support metrics to help IT management optimize decisions and accelerate the alignment of IT with business goals. Look for a dashboard solution that includes best-practice metrics and KPIs aligned with ITIL best practices and that does the following:

- Leverages a highly intuitive, graphical interface with right-time metrics aggregated across IT processes
- Enables a cross-functional view of IT
- Provides "just enough" drill-down, as well as trending capabilities across business services
- Supports fully customizable, personalized, and role-based views for KPIs
- Provides useful reports for decisions, instead of reports just for the sake of reporting
- Integrates with a service knowledge management system architecture

Look for an IT service management solution that integrates the service desk application with incident, problem, change, asset lifecycle, and service level management applications.

Solutions That Support Service Transition

The second category of IT systems includes the service management tools and technology to perform data mining, database management, release and deployment, publishing, and more.

Improving Efficiencies and Service Quality Through Knowledge Management

The *Service Transition* publication discusses knowledge management in the context of document management, records management, and content management. Knowledge management is also useful in other contexts, such as in the call center and on the service desk. Call center efficiencies can be dramatically

improved by providing agents with quick answers and solutions to their customers' issues. In addition, Web-based self-service options allow employees or customers to find their own answers 24x7, using natural language search, which can significantly reduce the number of issues directed to a service desk.

Look for a solution that provides the following features:

- Rich HTML authoring to deliver best-practice authoring with extensive, rich-text HTML editing tools
- Searching and security features to enable users to search across multiple sources using natural language query
- A self-help capability to allow users to search for their own solutions and create their own trouble tickets
- Enforceable authoring process and notifications to ensure, in a timely manner, that the knowledge is consistent and up to corporate standards
- News flashes and watch lists so users can see important notices and learn about changes or new solutions created in their category of interest

An Interdependent World

Today's workplace is an interdependent environment. Colleagues, customers, and suppliers around the globe share calendars, send instant messages, exchange emails, and use technology in a number of ways that increase collaboration and productivity. The DIKW model that was mentioned earlier is essential for decision support and should be architected in an SKMS fashion to enable stakeholder collaboration using the same data sources from the CMDB or CMS.

One way in which groups from disparate locations are coming together is in online communities. Communities provide a forum in which members can share ideas, projects, or other knowledge assets. Recognizing and rewarding members for their contributions can foster the free exchange of knowledge.

Automating Processes in a Changing Business Environment

Workflow management allows you to manage knowledge assets as they move through a specific process. An example given in the *Service Transition* publication is a request for change (RFC), which moves through a defined process from creation to release and deployment.

Look for a workflow management solution that provides a consolidated service process management platform for automating and controlling service management business processes, as well as a request-centric, workflow-based architecture. An effective system should also include prebuilt modules for notifications, escalations, and approvals, as well as the ability to monitor business activity to proactively measure business process performance.

Connecting Technology, Process, and Organization

Although the *Service Transition* publication does not specifically mention run book automation, it deserves mention in a discussion of automation.

Run book automation solutions enable you to streamline IT operations by automating routine, labor-intensive, error-prone tasks and by leveraging systems, applications, and tools across silos — from trouble ticketing to fault management to performance monitoring to virtualization management to the CMDB. They also help you automate release and deployment tasks. Managing across silos is a key focus of ITIL V3. As such, a comprehensive run book automation solution should provide out-of-the-box, ITIL-based process workflow to help you automate these manual, repetitive processes.

By uniting management systems and technologies with best-practice ITIL processes, run book automation delivers a unified service delivery capability.

By uniting management systems and technologies with best-practice ITIL processes, run book automation delivers a unified service delivery capability. Run book automation not only overcomes the barriers of technology, process, and organization (people), but also unifies the parts to work together efficiently and provide dependable service delivery. Once the links are established among technology, process, and organization, you can then begin to view the services you deliver to the business as just that — services — rather than focusing on the individual components. When you start looking at the services as a whole, you gain a better understanding of the end-user perspective. For example, the end user really only cares that the service is available and working as expected, and that's what IT needs to measure. If the sales order application isn't functioning, it doesn't matter if all the individual infrastructure components supporting it appear to be working properly. To the end user, IT has failed. ITIL provides a framework for adopting a service lifecycle approach and proper business perspective. IT then needs to establish service levels in accordance with business priorities to most effectively allocate resources (both people and technical resources) to the areas that matter most.

Run book automation solutions provide monitoring and measuring capabilities so that you know how the automation is affecting the overall process. This also enables you to adopt a continual service improvement program, another cornerstone of ITIL.
— excerpt from "Run Book Automation Sets the Stage for Business Service Management," *VIEWPOINT, Focus on: Service Automation*, published by BMC Software, 2007

For a more thorough list of systems that support service transition management, refer to Chapter 7 of the *Service Transition* publication.

The Importance of a Configuration Management System

A variety of additional tools are available to support effective service transition. The following ITIL definitions are key to this discussion: *configuration item (CI)*, *configuration management database (CMDB)*, *configuration management system (CMS)*, and *service knowledge management system (SKMS)*.

ITIL recommends using a software CMS to track the characteristics and history of each CI. The CMS can be fully automated, which may require the integration of multiple tools. The CMS prevents changes from being implemented without the proper authorization.

Most likely, you are trying to enable business growth (or at least not get in the way of it), and actionable information is the key to that growth. The core function of the CMS is to provide actionable data.

Figure 2 describes a sample SKMS. The CMS is a component of the SKMS. Note that this figure incorporates the DIKW methodology, which was discussed in Chapter 4 of this booklet.

A CMS may include various IT management tools, as well as databases — such as an asset database, a change management system, or a CMDB. It's up to you to decide what type of configuration you want for your CMS.

To look at the CMS in more everyday terms, think about the options available when you purchase a car. In most cases, you choose a standard model and then select add-on options or packages, such as leather seats, a sports rack, or a navigation system.

The process is similar when implementing a CMS. You get the standard model and add other components according to your own requirements. Taking the analogy a bit further, the CMDB is to the CMS as the engine is to your car. The CMDB is the core database that powers the complete CMS system.

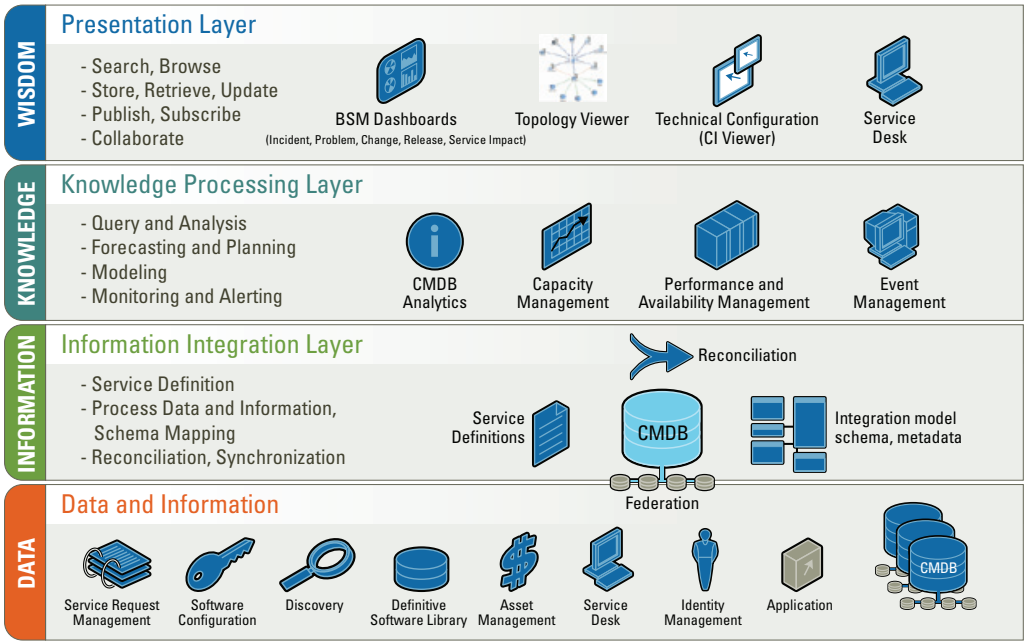


Figure 2. Sample Service Knowledge Management System (SKMS)

To understand the full value of a CMS, first consider the role and importance of a CMDB. A CMDB is a repository of information that relates to all the components, or CIs, associated across the IT environment.

Providers of IT management solutions offer commercial CMDBs to hold configuration data and make that information accessible to the management applications that need it — whether the application is a data provider or a data consumer. The CMDB provides a single point of reference, making it the definitive reference mechanism for all IT decisions. It provides business-aware visibility into the dependencies among business processes, users, applications, and underlying IT infrastructure.

The leading CMDB solutions are built to support a federated CMDB approach, meaning that not all configuration data must reside in a single physical database. The concept of federation relies on the premise that the CMDB should contain only needed data, while still being able to do its job. Other data sources and systems can be related to or federated to the CMDB without putting all the information within the CMDB itself. In fact, ITIL V3 now recognizes the importance of this federated approach and recommends that it be a core part of the structure of a CMS.

The CMDB provides a single point of reference, making it the definitive reference mechanism for all IT decisions.

With federation, core data is stored in the CMDB, just as information about a person or a business can be stored in a telephone directory. Then, all detailed and related CI data are federated, which simply means that a centralized database is linked to other, more detailed data stores. This linkage provides a CMDB access to the entire library content (the CIs). Hence, the CMS includes the CMDB or multiple CMDBs and, through federation, provides access to all primary data stores and their respective contents, thus providing a normalized single source of truth for organizational business decisions.

The core function of the SKMS is to help IT organizations solve problems or make decisions from the collaborative business perspective. By ensuring all IT management applications have access to properly cataloged IT configuration data, the SKMS can provide you with the insight necessary to make improved business decisions. This approach is known as Business Service Management (BSM), another best practice featured in ITIL V3. BSM solutions, when deployed effectively, dynamically guide IT actions and decisions according to their impact on business services. They should provide out-of-the-box support for best-practice IT processes, automated technology management, and a shared view of how IT supports business priorities.

Eliminating Manual Effort Through Auto-Discovery

Although the *Service Transition* publication does not provide details on discovery, here are some things to think about.

Discovery solutions can enrich the CMDB by automatically discovering people, business processes, applications, and IT infrastructure data to provide an up-to-date picture of your IT environment, the people who depend upon it, and the business processes that make up your critical business services.

An effective discovery solution will have out-of-the-box integrations to populate and maintain your CMDB. It should have the capability to discover dependencies in three main areas:

- *People discovery* auto-discovers end users and customers to establish dependencies from people to business processes, applications, and IT infrastructure.
- *Business process discovery* auto-discovers business processes and services to establish a link from processes to people, applications, and IT infrastructure.
- *Application and infrastructure discovery* auto-discovers the applications and IT infrastructure, identifies resources for deeper collection of configuration information and application dependencies, builds relationships between IT infrastructure resources, and establishes the link from IT to people and business processes.

Prioritizing IT Events Based on Their Business Impact

IT managers need real-time business-aware information about IT services and infrastructure. Service impact management solutions leverage existing management tools and process events against service models that relate IT and the business. Business-aware service models enable IT to pinpoint root causes and prioritize business-critical problems. Service impact management uses the CMDB as an instrumented asset and configuration data source to create and maintain models. Common reporting and Web portal technologies deliver role-based dashboards and IT service impact reports.

IT managers must understand how the IT infrastructure relates to the business services that IT provides. A solution that shows a graphical representation of the relationships within your IT infrastructure will enable BSM through real-time business-aware information about IT services and infrastructure. An effective solution will leverage existing management tools and will process events against service models that relate IT and the business. Your solution should integrate with your CMDB and provide reporting and dashboard capabilities.

Look for a solution that has the following features:

- Shows the real-time impact of IT problems on IT and business services through real-time service views, dashboards, and reports
- Promotes organizational knowledge of the value of IT to the business and the importance of services to business operations
- Instruments the creation and maintenance of models through the CMDB, a repository for discovery, change, asset, and configuration data
- Extends the value of existing IT tool investments through the CMDB and by leveraging events from existing management tools

Reducing Costs Through Release and Deployment Technology

Managers responsible for release and deployment must do the following:

- Provide IT efficiency
- Improve service quality
- Offer a secure and compliant environment
- Provide comprehensive scenario planning
- Prepare stakeholders for change with training

Release and deployment technology reduces both desktop administration and server configuration costs, as well as improves risk management and employee productivity. Look for a policy-based solution that automates the discovery, packaging, provisioning, configuration, patching, and repair of software. A comprehensive release and deployment solution will enable you to be less dependent on multiple software distribution tools.

Figure 3 illustrates and describes one example of the process by which release and deployment technologies provision a new service. Release and deployment technology is often referred to as *service automation* or *service provisioning*.

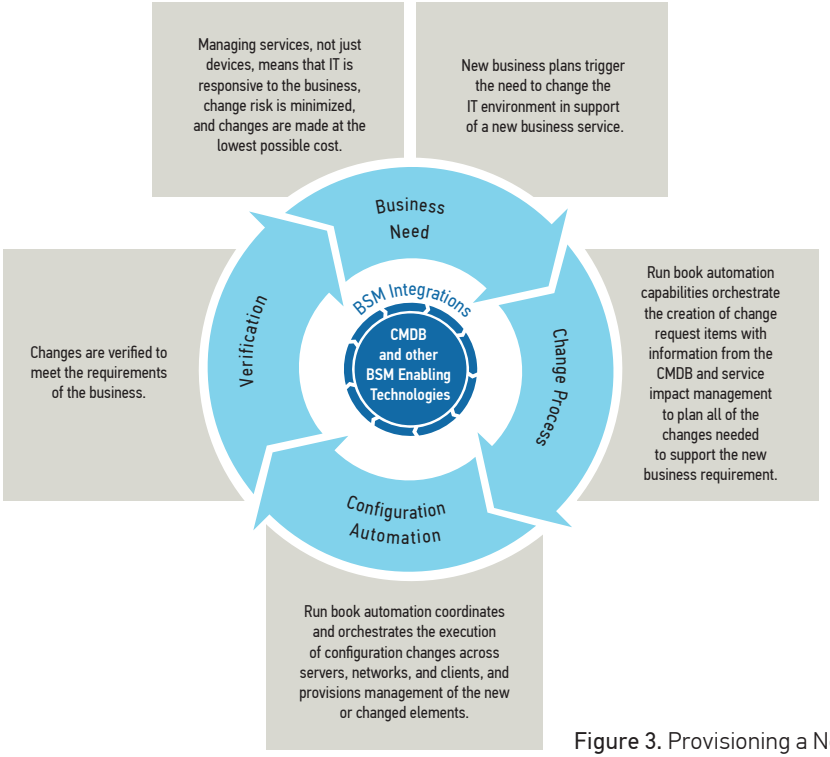


Figure 3. Provisioning a New Service

Summary

Change, configuration, incident, and problem management systems must support service transition. Whatever tools you select, they should be part of an integrated suite. That's the best way to gain the BSM context necessary to link CIs, and to understand the relationship between those CIs and the services they support. This business-centric view is necessary to effectively prioritize risk, as well as response to incidents, problems, and proposed changes.

Whatever tools you select, they should be part of an integrated suite.

Change Management

Think of change management in terms of risk management, and think of the SKMS, CMS, and CMDB in terms of decision support and as the central nervous system of an IT organization. Yet, the areas the SKMS, CMS, and CMDB touch also go well beyond IT and into the business — they extend to all the stakeholders in most projects and programs.

Configuration Management

An SKMS, CMS, and CMDB can embody knowledge that allows you, at the top level, to identify a service that may need to demonstrate compliance with regulations such as Sarbanes-Oxley. Your SKMS, CMS, and CMDB can help you trace the entire lineage of the supporting infrastructure, assets, and other pieces, so that you can build an adequate system of controls around them. The business should have input to identify the services, but IT should be the one to connect and maintain the services inside the system.

Incident Management

When the service desk receives a call about an outage, the first thing the agent will probably do is look at the changes that were planned and have been implemented in the past 24 hours. Most incidents occur after a change has been implemented. If you allow service agents to access that change information from the service desk, you can gain a tremendous benefit by pinpointing the most likely cause of the incident. You can use the SKMS, CMS, and CMDB to see information about the pieces in the infrastructure that changed and use that information to quickly pinpoint the likely cause. This approach should reduce your outage time, simply because you're much more effective at isolating the actual cause, and then you can bring the system back up more quickly.

Problem Management

Data from incident and problem management can help you prioritize changes in the change management process. Suppose you've identified the root cause of a problem, then someone proposes a change to remove

that root cause from the infrastructure. As you are evaluating the change and trying to prioritize it, ask yourself: *Is this something we have to do now, or can it wait? How essential is it? Is that root cause actually causing outages, or is it simply annoying to users? What is this about, what service is affected, and how business critical is that service?* You also should be able to look at that problem and then look at all the related incidents. That perspective gives you an idea about the frequency with which this root cause is actually causing incidents.

Find out which patterns of business activity generate the most value, instrument that, adopt a BSM approach, put your SKMS, CMS, and CMDB in place, and then start to reap the benefits of service continuity and stable operations. That is the key. Get the big benefits, and you'll soon win the stakeholders over to this better way of managing IT.

Chapter 8
Implementing Service Transition

Since most companies are not starting from scratch, this chapter addresses service transition implementation from a process or service improvement angle. This will require an honest assessment of your current organizational capabilities that align with the service transition process. You probably have some — or even several — of these capabilities in one fashion or another. The challenge will be figuring out what business benefits can be delivered by managing discrete activities as a lifecycle. The ITIL *Continual Service Improvement* publication provides considerable guidance for just that type of process.

The stages of service transition adoption will parallel other organizational improvement efforts. There is a strategy element, followed by a design phase, service introduction, and then organizational adoption. Sounds a lot like the ITIL lifecycle doesn't it?

Introducing and Justifying Service Transition

Many IT organizations have difficulty estimating how much time they spend to transition a service into production and, then, to keep the service up and running. One reason for this is that large services are often developed

and run as a project from external consultants. Then, it's the job of the transition team to roll that service into operation. Most consultants will give you a fixed price to design and develop a service, but not to roll it into production. In rollout, you experience a lot of unanticipated touch points, and this is where delays and overruns typically happen. Until you have finished rolling a new service into operation, it's difficult to estimate how much time will be needed to maintain it. Realize that rollout will likely take much longer than you expect it will, and proactively plan for a greater expenditure of time and money than you originally estimated. A good SKMS is a critical success factor here.

In many cases, the time it takes to transition a service into production is actually tracked as part of a project; it is the "keeping the service up and running" part that is almost never addressed. If an IT organization already has that visibility internally, then the discussion with the business becomes much easier. Think about the following: *How much time am I spending on incidents, problems, and changes for each of the services? What do I plan to do with the services? How can I make IT work together from a resource perspective?* Many organizations can't answer these questions yet. When they change one service, they don't fully understand the potential impact on another service.

Being proactive means identifying weaknesses in your infrastructure *before* they cause service outages.

In chaotic environments, where customers tell IT that speed is the most important thing, yet IT has few resources, little budget, and a small staff, IT can consider two approaches: firefighting and fire prevention. In the first approach, your house is on fire and you have to put it out. While firefighting, you can adopt some very simple processes to reduce chaos. A good, reactive change management process is key to reducing chaos and getting your fire under control, but you can't do that unless you have integrated your operations with incident management and problem management. When you have achieved that integration, then you can start the proactive approach of fire prevention.

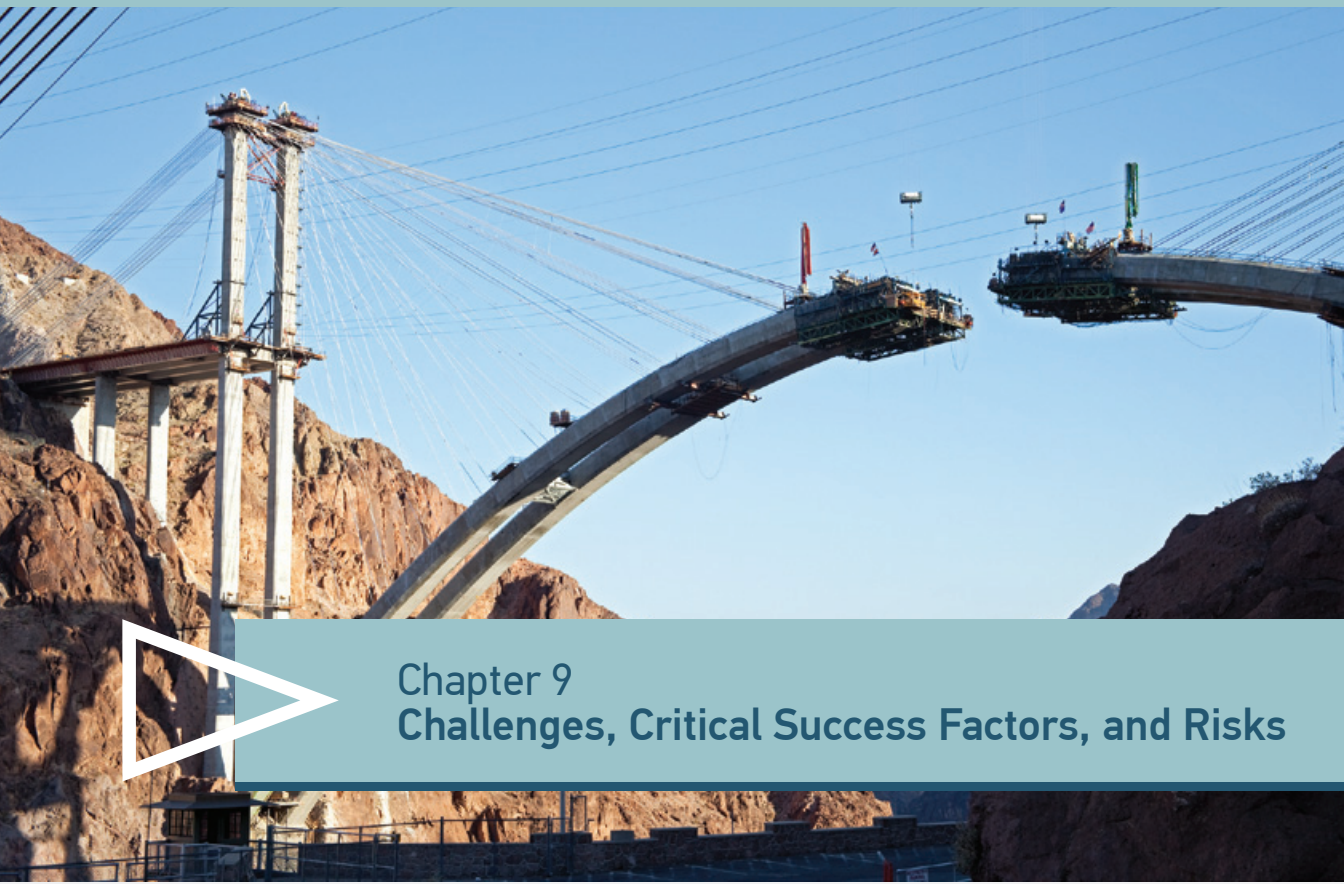
Being proactive means identifying weaknesses in your infrastructure *before* they cause service outages. Building effective change management can help prevent unplanned outages, because the reality is that 60 to 80 percent of all unplanned outages are caused by unauthorized and poorly conceived changes. Even organizations with minimal budgets can benefit from implementing these processes; a 25 percent reduction in overall operational costs is an achievable goal. This reduction or cost savings can result in an investment back into the business for growth.

Little by little, you should be able to put out the fires and start preventing them. But if you don't have any capital to do so, it is a much slower and more painful process. If you have capital to help you cool the fires, then you can start working on prevention. In private enterprises, a chaotic system usually has negative

implications for revenue and profit, so justifying the investment in change management is easier when you can show a return on investment. In government agencies, the motivation is not profit but, instead, reducing costs and maintaining a good reputation. Using the ITIL service lifecycle can help achieve both goals.

Summary

A thorough understanding of the unique needs of your company is the starting point for justifying service transition activities. Give your organization permission to take an honest look at problems and issues that have occurred during the past from the perspective of the business. Use these case studies to justify the service transition approach to delivering value, and you will be more likely to create a sense of urgency in the organization and engage business executives in a meaningful conversation about providing funding and cooperation.



Chapter 9
Challenges, Critical Success Factors, and Risks

In many lines of business, such as e-business, IT not only supports business operations, it also *is* a business operation. Services can become very complex when all of the suppliers, third-party outsourcing agreements, and any international aspects are considered.

During service transition, most business processes and services are already IT-enabled; therefore, every IT change has potentially huge ramifications for the business. Service transition requires a myriad of communication points, relationships, and process handoffs that range from end users to suppliers. The service delivered must be in line with real business needs.

Risk has to be balanced against the return to the business. Project timeline slips and cost overruns in earlier lifecycle stages may threaten to eat into the time and budget allocated. When that happens, testing may get cut; but cutting testing increases your risk. To prevent this from happening, try to get more budget and time to ensure successful transition into operation.

Risks and Responsibilities

The beauty of service transition is that you can calculate the risk of every change before making it. You might follow one process for a change that has high risk and high return, and a different process for a low-risk, low-return change. Risks are not always negative; risk can be avoided, exploited, or accepted for business value.

A standard change is a low-risk, preapproved change in which most everything can be preprocessed. The high-risk change takes a different path and methodology. Build a triage process, so you can distinguish between the two types of changes. That is the intention of service transition. After the early decision by the business that an implementation could have a high return but also carry high risk, then it is the transition team's job to quantify that back to the business, so they can make the right business decisions.

> Risk has to be balanced against the return to the business.

Summary

Perform a business impact analysis with every major change, so you can estimate the cost of failure and anticipate the impact to the business. Follow a low-risk, high-yield return as much as possible when performing change management.

Afterword

BSM helps to ensure that the resource investments you make to bring new services online (or to change or retire existing services) are linked to business value and prioritized according to value. Through a BSM approach, you will streamline service transition activities and ensure that the quality of service necessary to achieve the desired business value is delivered. For example, your change management process will now include vital information about business impact, so that all responsible parties who authorize a change are fully aware of its implications.

Here are some keys to realizing the value of service transition:

- Assess the current change management process, identify gaps, and address the gaps for business value by using ITIL best practices.
- Start with a limited subset of business-critical services. Don't do a big bang approach by trying to do everything at once; remember, it's best to swallow an elephant one bite at a time.
- Map your service transition into the expectations and desires of the business. Establish metrics, so you know if improvement occurs. Focus on the business outcome from a value standpoint at every step of the way; for example, *I am going to perform X so that I get (insert business desire here).*

- Keep change management simple. Measure only the items that you can control. Focus on volatile services and fragile infrastructure components at first.
- Create a strong culture of change management. It must be clear that unauthorized change results in consequences for everyone. Create a solution adoption program that consists of communication, training, and celebrations of success.
- Implement a configuration discrepancy system to fulfill change management. This way, you have a baseline for all critical and fragile services and infrastructure so you can fall back in case of a failed rollout.

Service Transition and BSM

Without BSM, it is nearly impossible for IT to quantify the business value or impact of what IT does. IT can work with all of these processes and streamline everything, but if you don't know what the business really needs and wants, and if you cannot link the IT work back to a business impact, then you're unlikely to meet the business's requirements. And your ROI will be minimized because you don't really know how to prioritize for optimum business return.

> Through a BSM approach, you will streamline service transition activities and ensure that the quality of service necessary to achieve the desired business value is delivered.

For example, provisioning a service with a BSM approach allows you to be responsive to the business while minimizing both cost and risk. When you are planning a new service, this activity triggers the need for a change in the IT environment. With a comprehensive BSM solution, the change request items are automatically meshed with information from the SKMS, CMS, and CMDB as well as service impact management. Run book automation then coordinates all of the changes across servers, networks, and clients, and provisions the management of the new or changed parts of the service. Changes are verified to be sure they meet the requirements of the business. The cycle continues, as new business needs arise in response to the previous changes. By managing services holistically, instead of managing the individual components that support the service, you will be responsive to the business.

From Launch Pad to Liftoff

You can't send a spacecraft to Mars without making some adjustments along the way. And any new or improved IT project may have a few glitches. But, a solid service transition process can help mitigate or even prevent their impact. It can keep all stakeholders informed and engaged. And, it will ensure a safe liftoff as the IT project enters its service operation stage, where business value is realized.

This publication was created by BMC Software.

Business Runs on IT.
IT Runs on BMC Software.
Business runs better when IT runs at its best. That's why more than 25,000 IT organizations — from the Global 100 to the smallest businesses — in over 120 countries rely on BMC Software to manage their business services and applications across distributed, mainframe, virtual and cloud environments. With the leading Business Service Management platform, Cloud Management, and the industry's broadest choice of IT management solutions, BMC helps customers cut costs, reduce risk and achieve business objectives. For the four fiscal quarters ended December 31, 2011, BMC revenue was approximately $2.2 billion. Visit **www.bmc.com** for more information.

A BMC Software Education Services publication