John Long

ITIL® Version 3 at a Glance

Information Quick Reference

Springer

ITIL® VERSION 3 AT A GLANCE

ITIL® VERSION 3 AT A GLANCE

Information Quick Reference

John O. Long
IBM

Springer

John O. Long
IBM
P.O. Box 12195
Research Triangle Park, NC 27709
j1long@us.ibm.com

ISBN: 978-0-387-77392-6 e-ISBN: 978-0-387-77393-3
DOI: 10.1007/978-0-387-77393-3

Library of Congress Control Number: 2007941324

© 2008 Springer Science+Business Media, LLC
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Copyright and Legal Information

ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

ITIL® Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce.

This book is currently under consideration by publishers. This book may only be distributed by the author for evaluation purposes.

Table of Contents

Introduction

Purpose

The purpose of this book is a quick reference for ITIL® version 3. It is not intended as an overview of ITIL® version 3. It is suggested that you first familiarize yourself with the ITIL® version 3 documentation before using this book. This book contains references to more detailed material found in ITIL® version 3.

Audience

This book is intended to be used by anyone involved in planning, consulting, implementing, or testing an ITIL® version 3 implementation.

Organization of the Book

Each chapter in this book summarizes one of the core ITIL® v3 books. Each book in the ITIL® v3 series represents a single stage in the lifecycle of an IT service. The first and last books in the series, Service Strategy and Continual Service Improvement, do not contain rigorously-defined processes, but instead describe a set of practices that may be used during those stages of the service lifecycle. The second, third, and fourth books in the series, Service Design, Service Transition, and Service Operation, contain rigorously-defined processes.

The subsequent chapters in this book each summarize one of the ITIL® v3 books. The Service Strategy and Continual Service Improvement chapters contain the following structure:

- Brief Description of the Stage
- Overview Diagram of the Stage

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_1,
© Springer Science+Business Media, LLC 2008

- Key Concepts of the Stage
- Practices[1] or Processes[2]
- Roles[3]

Each process section within a chapter is structured in the following way:

- Process Purpose
- Overview Diagram
- Key Concepts

[1] For the Service Strategy chapter and the Continual Service Improvement chapter.

[2] For the Service Design, Service Transition, and Service Operation chapters.

[3] This section is missing for Service Strategy because no roles are described in the ITIL book.

Service Strategy

Brief Description

Service Strategy defines an IT organization's high-level approach to providing services. First, the IT organization must identify the market for its services. This, in turn, drives the identification of services offerings as well as the strategic assets that will constitute those services. Envisioned services will be added to the service portfolio. These envisioned services will continue to be pursued until they are finally chartered for design (and development), which moves those services into the Service Design stage.

Supporting this overall activity is the need to determine the IT organization's overall approach to providing services. This may include internal providers, external providers, a shared approach, preferred providers, etc. In addition, several practices play a part in determining the overall service strategy, including financial management, demand management, and risk management.

Practices

Primary Practices

Market Definition – Defining who the customers are for IT services.

Offering Development – Identifying services to be offered to customers and initiating projects to develop those services.

Prepare for Execution – Prepare the IT organization to be able to carry out the service strategy successfully, including identifying critical success factors, setting objectives, prioritizing initiatives, promoting growth, and differentiating the IT organization as a service provider.

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_2,
© Springer Science+Business Media, LLC 2008

Strategic Asset Development – Identifying assets that may be used as building blocks for the creation of services and initiating projects to develop those assets.

Supporting Practices

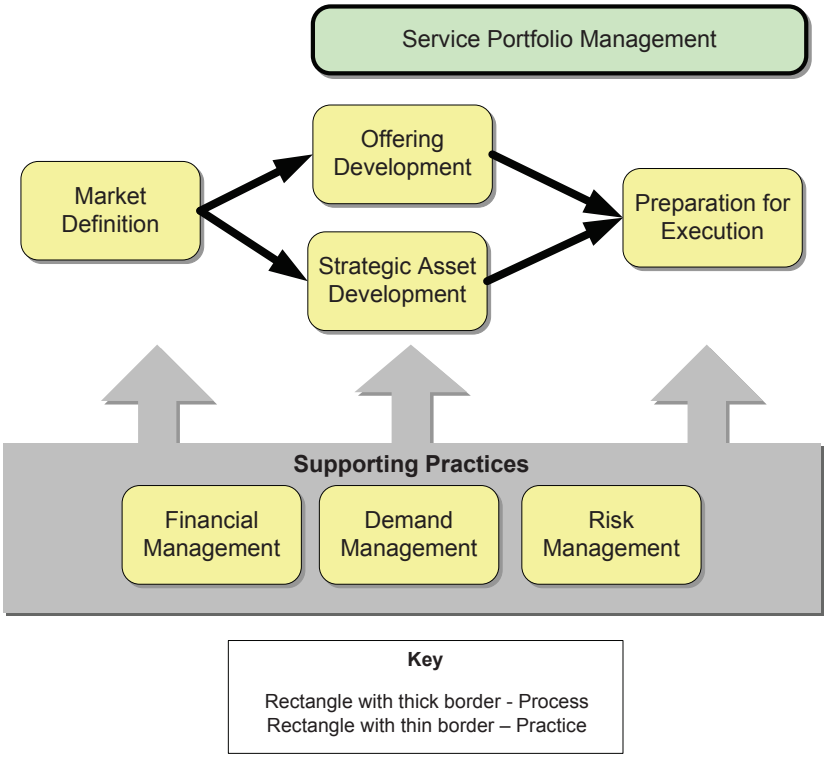
Demand Management – Promoting reduced demand for services as needed by the IT organization. This may include reducing user access, providing user incentives to reduce demand during peak hours, etc.

Financial Management – Managing the accounting, charging, and collection of fees for IT services.

Risk Management – Identifying, evaluating, and determining acceptable responses to risks.

Service Portfolio Management – Managing the list of planned, existing, and retired services.

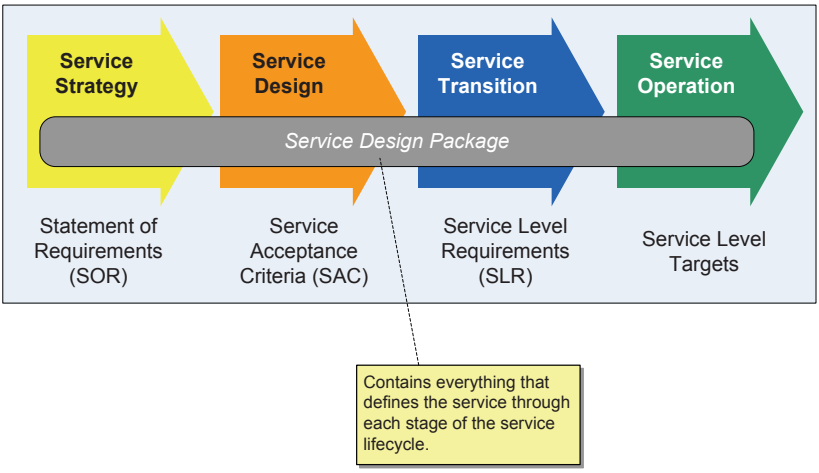
Overview Diagram



Service strategy defines a number of processes and practices

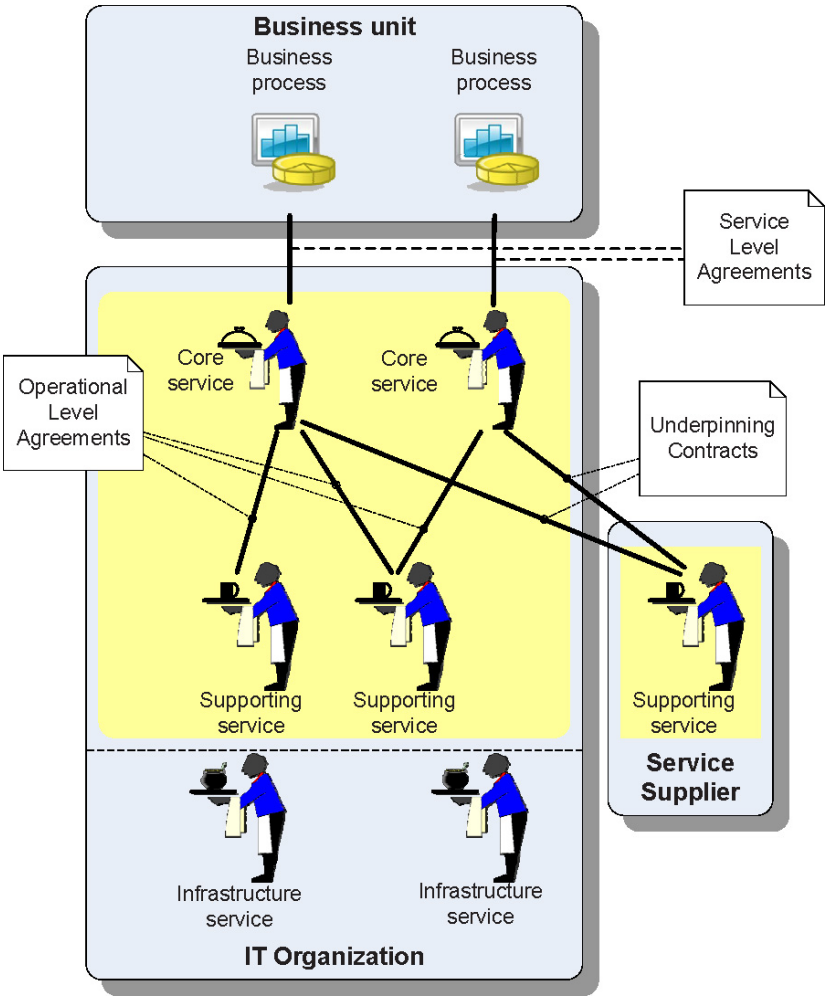
Service Strategy Key Concepts

Service Design Package and Other Service Artifacts



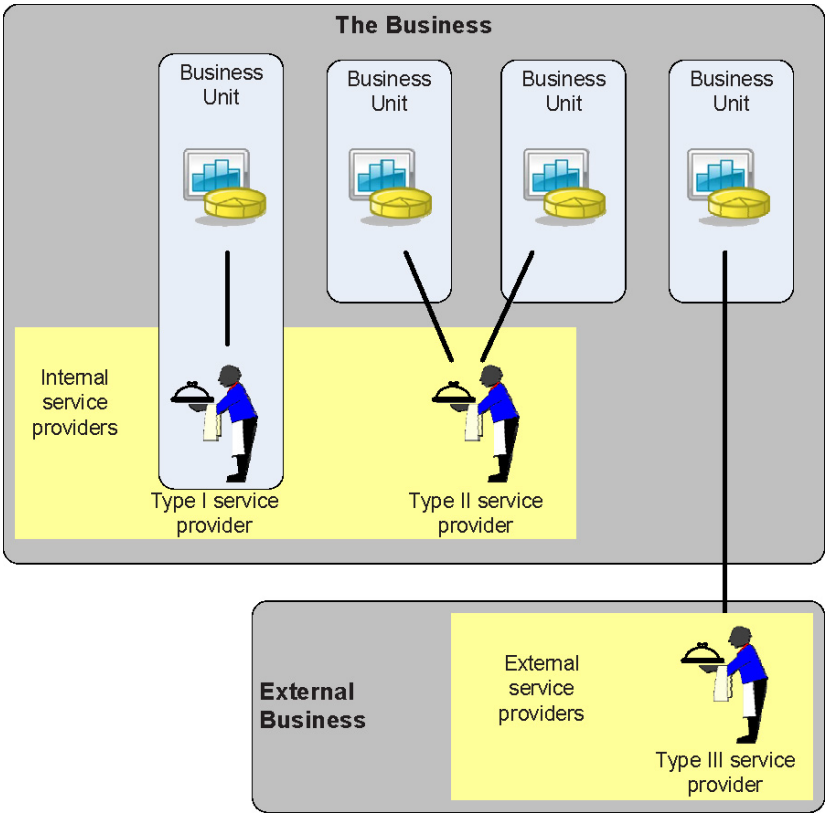
The service design package is used throughout the service lifecycle

Types of Services



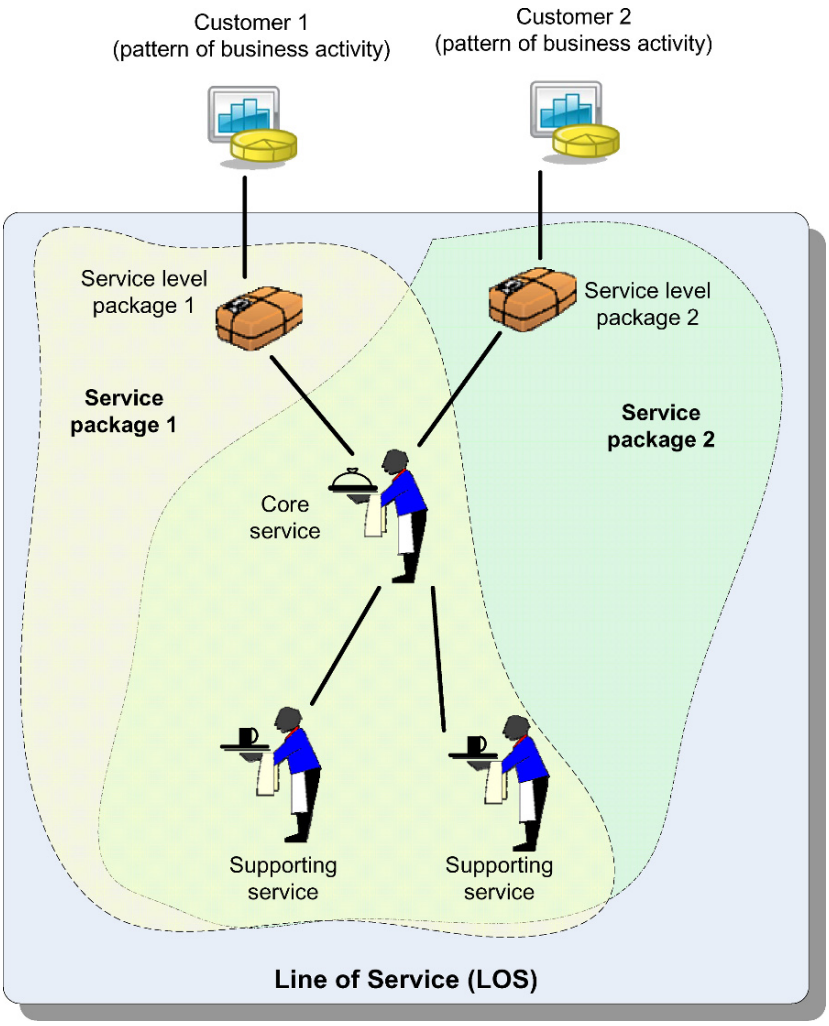
An IT organization provides core services, supporting services, and infrastructure services

Service Providers



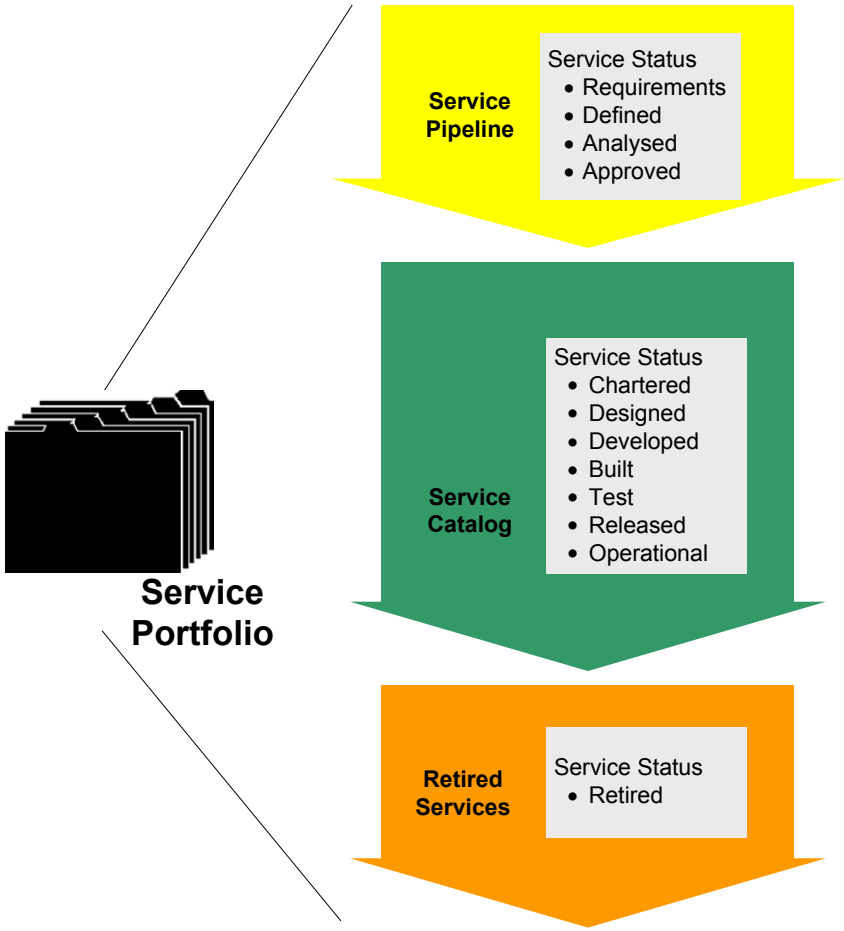
There are three types of service providers

Service Packages, Service Level Packages, and Lines of Service



A line of service consists of all service packages for a service

Service Portfolio and Catalog



The service portfolio includes the service pipeline, the service catalog, and retired services

Service Design

Brief Description

Service Design is a stage in the service lifecycle in which a new or modified service is developed and made ready for the Service Transition stage.

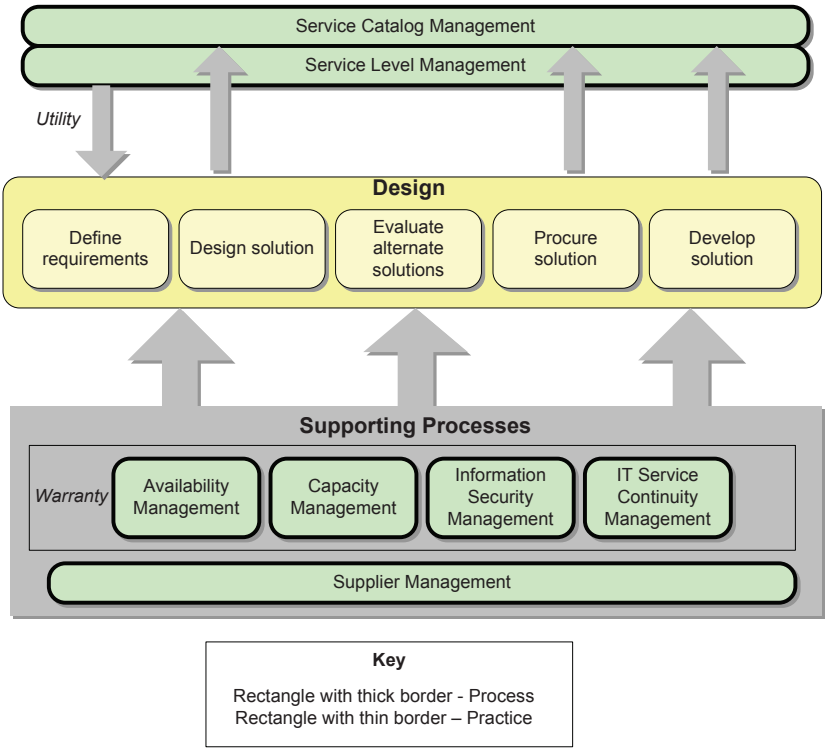
The primary effort of this stage is the design (and development) of the service. This includes defining service requirements, designing the service solution, evaluating alternate suppliers of the service, and integrating service assets into a service.

Service Level Management provides the interface to IT customers in the collection of requirements. Supporting processes such as Availability Management, Capacity Management, Information Security Management, and IT Service Continuity Management are consulted to make sure the envisioned service will meet service level targets and expectations. Supplier Management manages relationships with potential service providers.

As the service progresses through this stage, the Service Catalog is updated with new information about the service, including status changes in the service. The Service Catalog is that part of the Service Portfolio that can be viewed by IT customers. It is also an instrument of Service Level Management to enter into discussions with IT customers about new service requirements or about the initiation of a service level agreement.

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_3,
© Springer Science+Business Media, LLC 2008

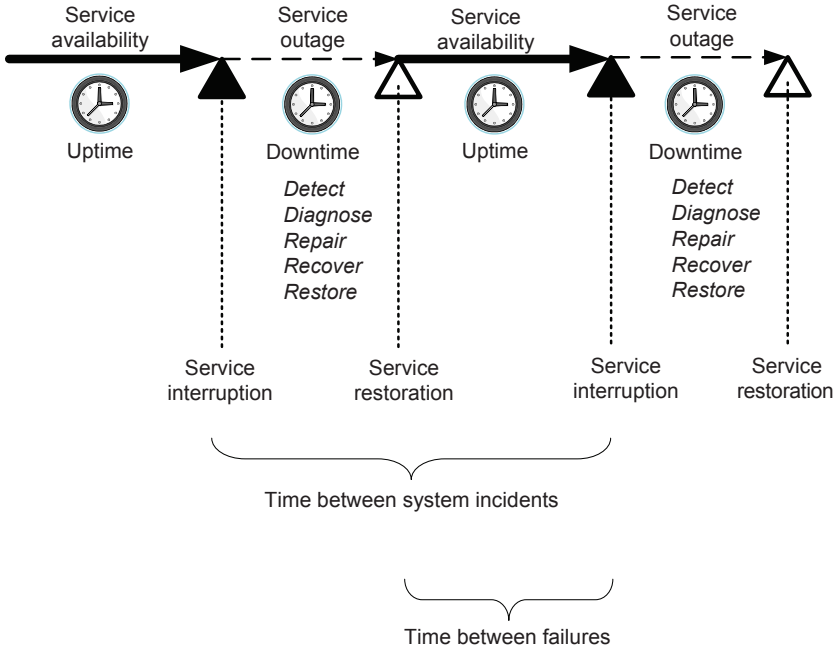
Overview Diagram



The design of services is at the heart of this lifecycle stage

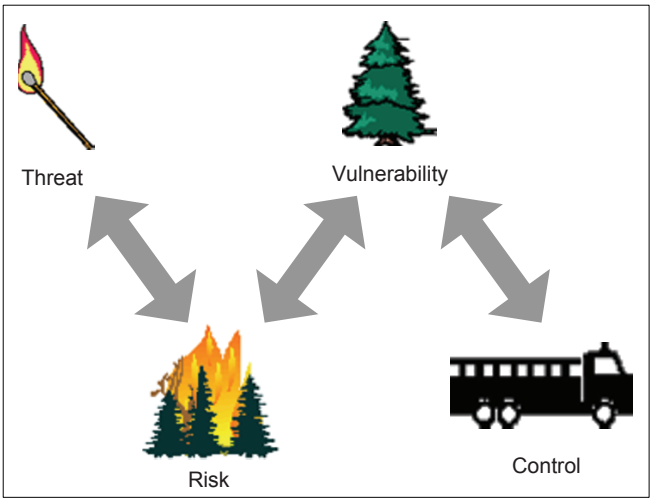
Service Design Key Concepts

Service Availability



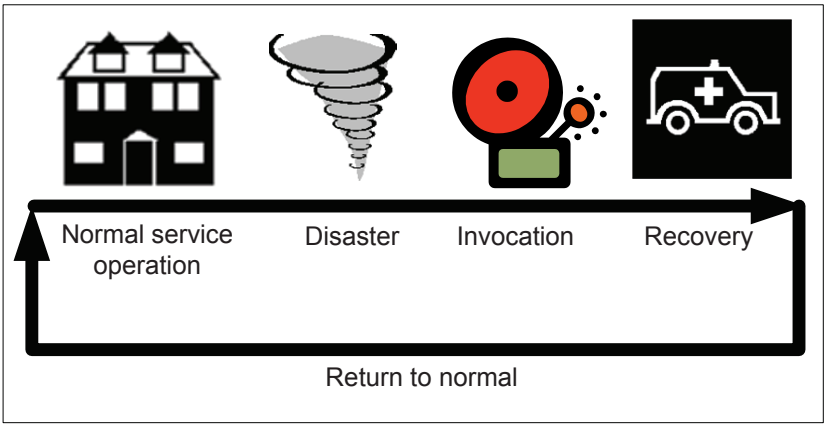
Standard metrics are used to measure service availability

Information Security



Information security involves identifying threats, vulnerabilities, and risks, and then implementing appropriate controls

Service Continuity



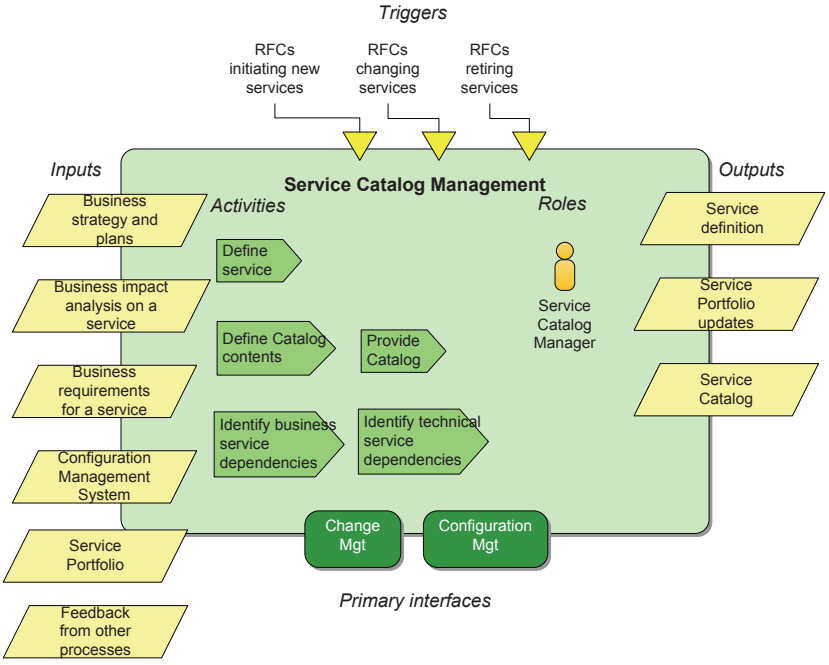
Service continuity is a cycle involving service operation, disaster, invocation, and recovery

Service Catalog Management

Purpose

Provide and manage a widely-accessible catalog of IT services.

Overview Diagram



Key Concepts

Business Service Catalog – The collection of IT services that directly enable processes that are part of the business.

Hierarchy of services – A network of services that support business processes (business services) and services that enable those business services (technical services).

Service – A collection of IT systems, components, and resources that work together to provide value to IT customers.

Service Catalog – The collection of IT services currently provided to IT customers.

Service Package – An in-depth description of an IT service available through the Service Catalog.

Service Portfolio – The collection of all IT services, including those in the pipeline, those currently being delivered, and those that have been retired.

Technical Service Catalog – The collection of IT services that support business processes.

Roles

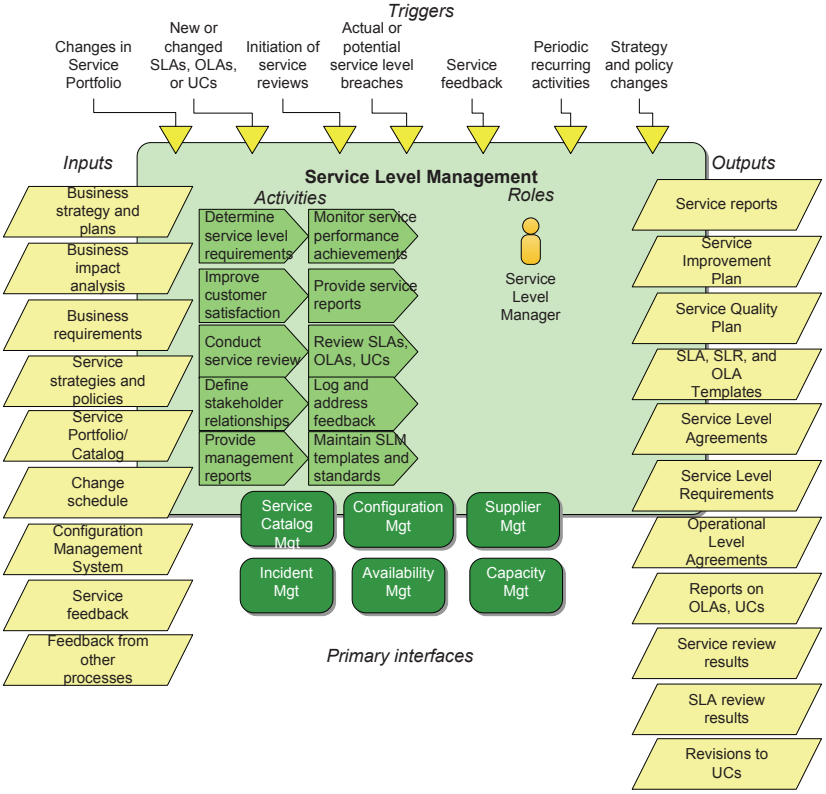
Service Catalog Manager – Maintains information within the Service Catalog and makes that information available to IT customers

Service Level Management

Purpose

Ensure that an agreed level of service is provided to IT customers.

Overview Diagram



Key Concepts

Operational Level Agreement (OLA) – An agreement with an internal service provider to provide services within specified levels.

Service Level Agreement (SLA) – A negotiated agreement between the IT service provider and the IT customer defining the responsibilities of each party concerning the delivery of an IT service.

Underpinning Contract (UC) – An agreement with an external service provider to provide services within specified levels.

Roles

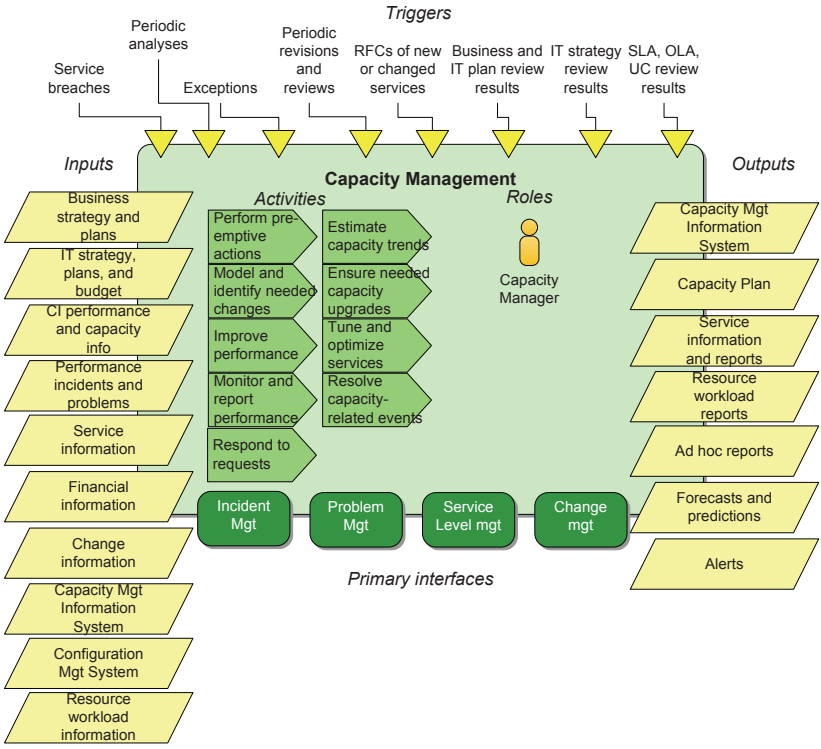
Service Level Manager – Negotiates Service Level Agreements and ensures that service levels meet or exceed service level targets

Capacity Management

Purpose

Provide a focal point for performance and capacity-related analyses and planning.

Overview Diagram



Key Concepts

Business Capacity Management – The management of capacity for business services.

Capacity – The maximum throughput that can be provided by a CI.

Capacity Plan – A long-term plan for providing adequate service capacity to meet expected service level targets.

Capacity Management Information System – The information system that contains all capacity-related plans, analyses, information, and reports.

Component Capacity Management – The management of capacity for configuration items that make up an IT service.

Demand – Desired use of an IT service or resource.

Human resource capacity – An aspect of Capacity Management that deals with staffing, scheduling, and training of human resources and their effects on service capacity.

Performance – The measurable results of a resource, CI, or service.

Service Capacity Management – The management of capacity for IT services.

Threshold – An operational level that, when exceeded, causes an alert or action to be initiated.

Tuning – The adjustment or manipulation of IT resources to make better use of those resources, including balancing and optimization.

Utilization – The use of a resource.

Roles

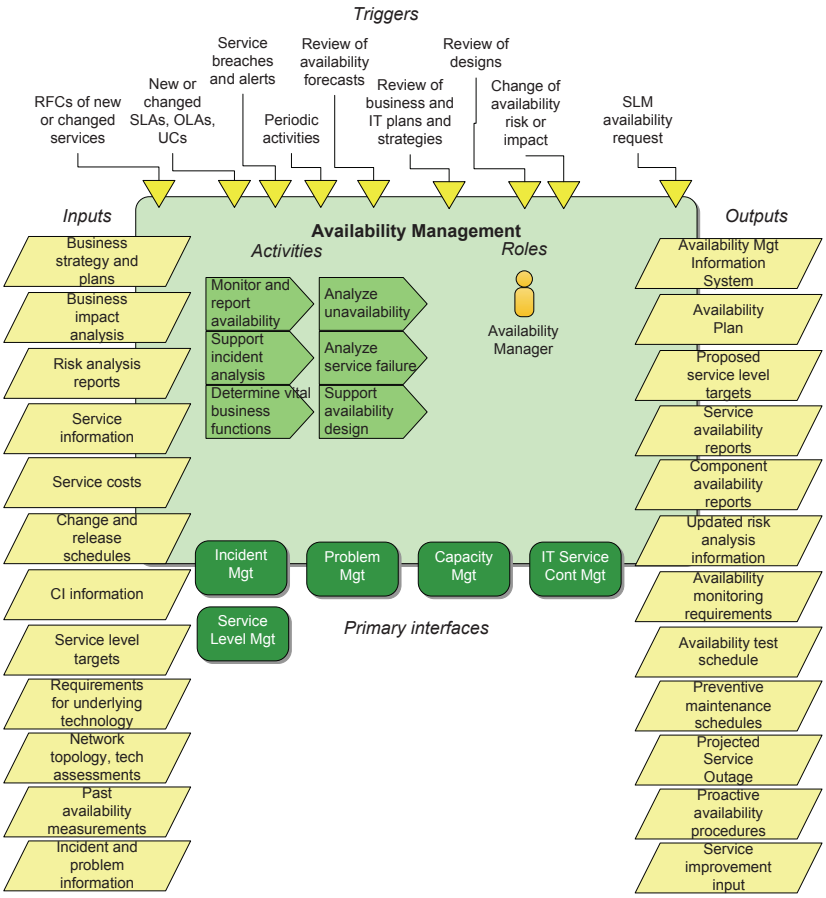
Capacity Manager – Oversees Capacity Management activities

Availability Management

Purpose

Provide a focal point for availability-related analyses and planning.

Overview Diagram



Key Concepts

Availability – The ability of an item to perform its function when required.

Component Failure Impact Analysis – Analysis performed to determine how component failure impacts IT services.

Fault Tree Analysis – Analysis that indicates a chain of events that led to a problem.

Maintainability – How rapidly an item can be restored to normal operation after a failure.

Reliability – How long an item can perform its function without interruption.

Service Failure Analysis – Analysis performed to determine the cause of related service interruptions. Note that this focuses on service interruption as opposed to Root Cause Analysis, which focuses on the cause of incidents.

Single Point of Failure (SPOF) – A configuration item that, when it fails, may cause an incident. Identification of SPOFs is an important aspect of managing service availability.

Vital business function – The critical business functions of a business service.

Roles

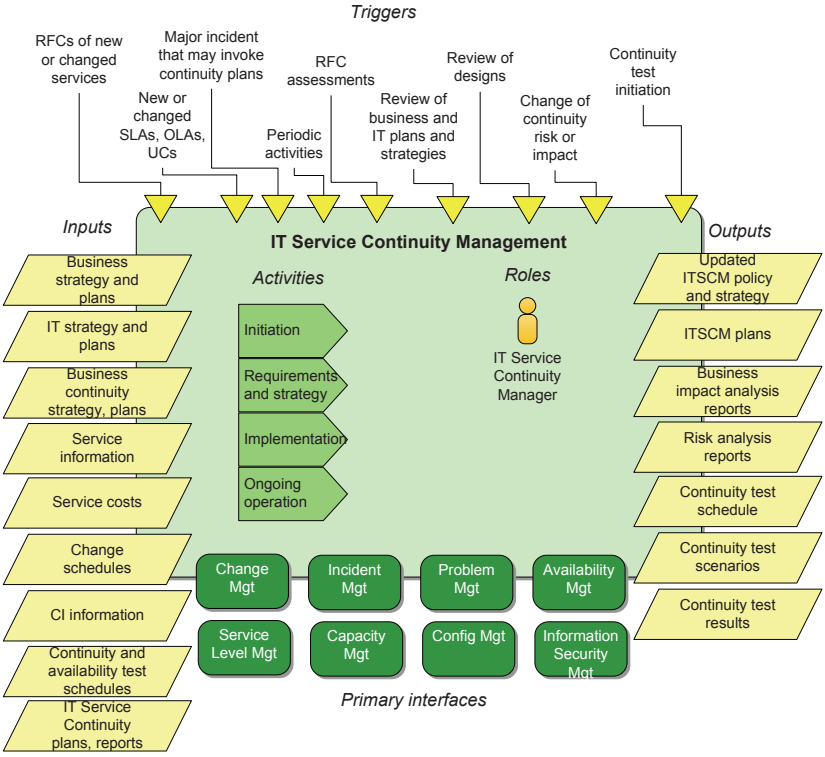
Availability Manager – Oversees Availability Management activities

IT Service Continuity Management

Purpose

Ensure that IT services will continue to operate according to an agreed-to plan.

Overview Diagram



Key Concepts

Business Continuity – Continuing to provide business services after a major outage. This is directly related to IT Service Continuity.

Business Continuity Plan – A plan to restore business services after a major outage.

Business impact analysis – An approach to determining vital business functions and dependencies.

Continuity testing – Performing tests of continuity plans to ensure that they will work in the face of a major outage.

IT Service Continuity – Continuing to provide technical services after a major outage.

IT Service Continuity Plan – A plan to restore IT services after a major outage.

Management of Risk (M_o_R) – A methodology to assess the impact of risks within an enterprise.

Restoration – Returning a CI or service to its normal operating state after repair and recovery.

Risk analysis – Determining the vulnerability to IT service threats.

Roles

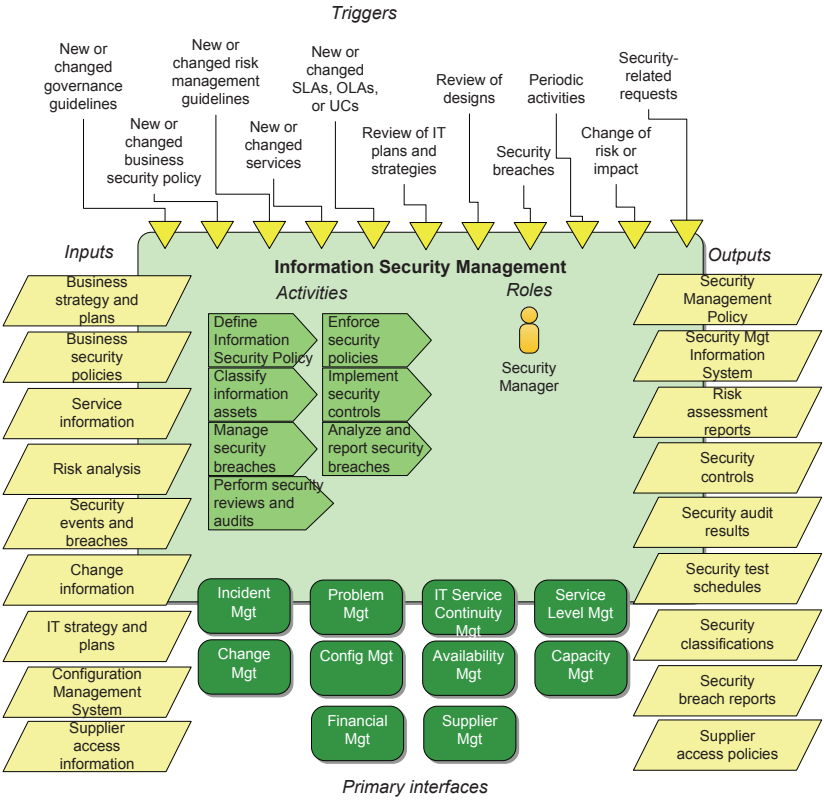
IT Service Continuity Manager – Oversees IT Service Continuity Management activities

Information Security Management

Purpose

Align IT security with business security.

Overview Diagram



Key Concepts

Information Security Management System (ISMS) – An information system containing information security standards, policies, and procedures.

Information Security Policy – An overall policy for conducting information security, supported by a number of underpinning security policies, including

- Access control
- Password control
- Antivirus policy
- Internet policy
- Asset use policy
- And others

ISO 27001 – International standard for certifying an ISMS.

Roles

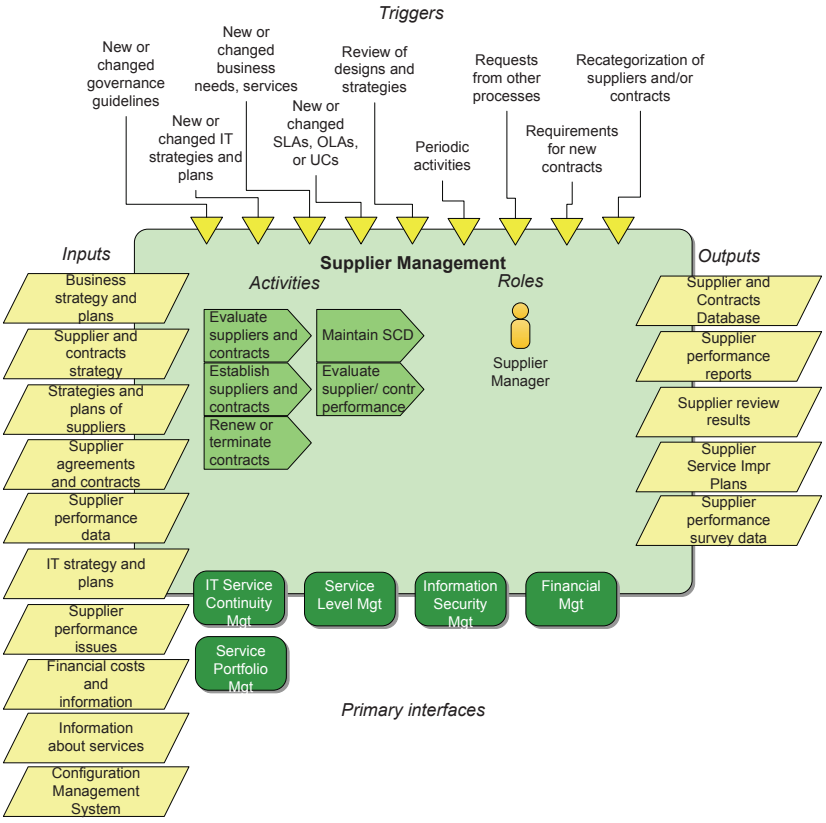
Security Manager – Oversees Information Security Management activities

Supplier Management

Purpose

Manage service providers in support of service level targets.

Overview Diagram



Key Concepts

Invitation to Tender (ITT) – A document similar to the Statement of Requirements.

Operational Level Agreement (OLA) – See Service Level Management.

Service Provider – Any internal or external provider of an IT service.

Statement of Requirements (SoR) – A document identifying all requirements for a service or project.

Supplier and Contracts Database – a repository of information about suppliers and contracts with suppliers.

Supplier performance – Suppliers that provide services at appropriate levels of service tend to be retained, whereas those that do not tend to have their contracts terminated.

Supplier Service Improvement Plan – Actions that are to be taken by a supplier to improve levels of service.

Underpinning Contract (UC) – See Service Level Management.

Roles

Supplier Manager – Oversees Supplier Management activities

Other Practices

Application Management – The management and control of applications through their entire lifecycle, from creation to retirement.

Data and Information Management – The control, organization, and disposition of data and information within the organization. This includes collection as well as disposal.

Design – The definition of an IT service based on collecting requirements, designing the service, and identification/ implementation of a service to meet those requirements.

Requirements Engineering – The discipline of collecting, organizing, and prioritizing requirements for a CI or service to be designed.

Service Portfolio Management - Managing the list of planned, existing, and retired services.

Additional Service Design Roles

IT Designer/Architect – Designs needed IT technology and coordinates those designs within the IT organization

IT Planner – Creates IT plans and coordinates them with other IT plans

Process Owner – Ensures process is being performed as documented

Service Design Manager – Ensures services are created as designed

Service Transition

Brief Description

The service transition stage readies a new or changed service for operation. The primary activity done during this stage is Transition Planning and Support. This process plans all of the activities that must take place to put the service into production. This may involve the creation of a number of RFCs that will carry out all necessary changes (Change Management) and deployments (Release and Deployment Management).

Prior to moving the service into production, there may be a period of testing and validating the service to ensure sufficient quality of the service.

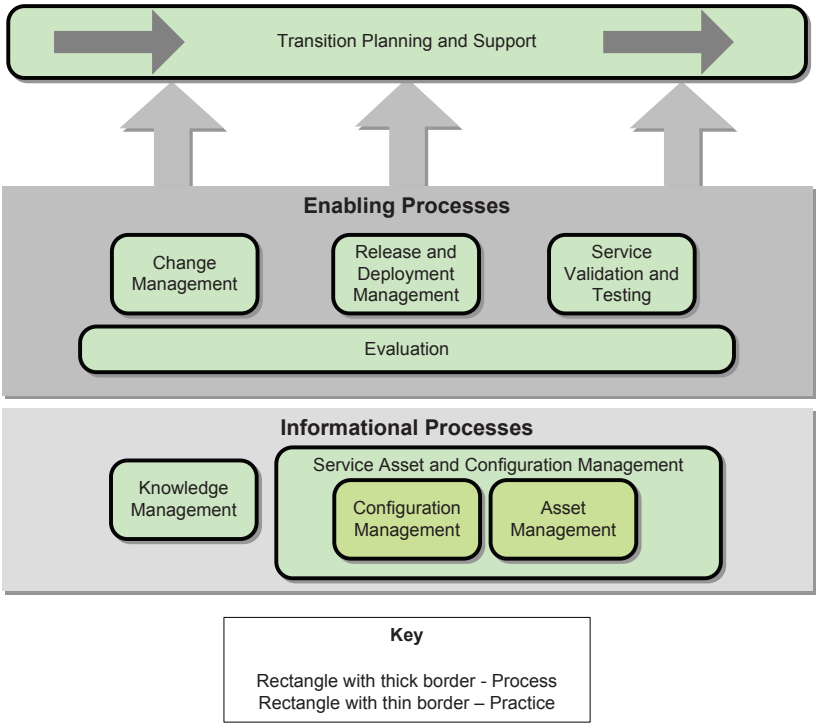
An overall evaluation framework is used by transition planning and support to determine if the service is still in an acceptable state to proceed or must be remediated in some manner.

As the service is readied for production, various configuration items and assets must be assembled and prepared. Information about all of these CIs and assets, as well as the relationships between all of these elements, must be maintained in order to provide the best support for the service.

Knowledge about the services and underlying CIs and service assets is collected during this stage and subsequent stages in order to provide effective support for service faults.

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_4,
© Springer Science+Business Media, LLC 2008

Overview Diagram

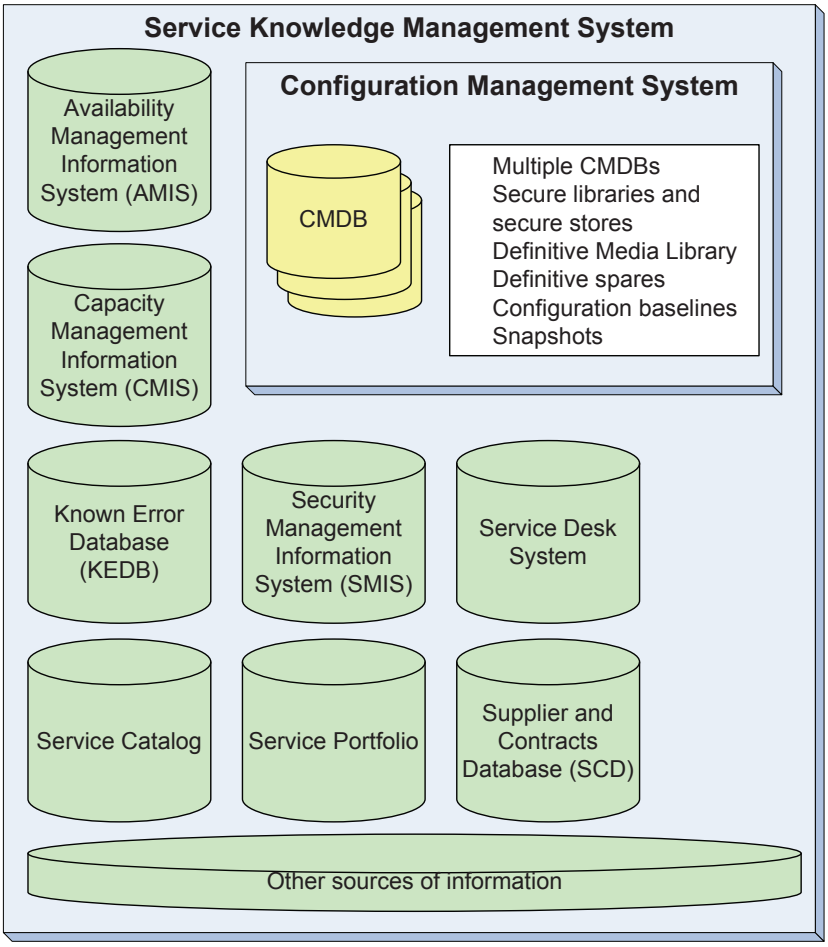


A number of enabling and informational processes support the transition of a service into operational status

Service Transition Key Concepts

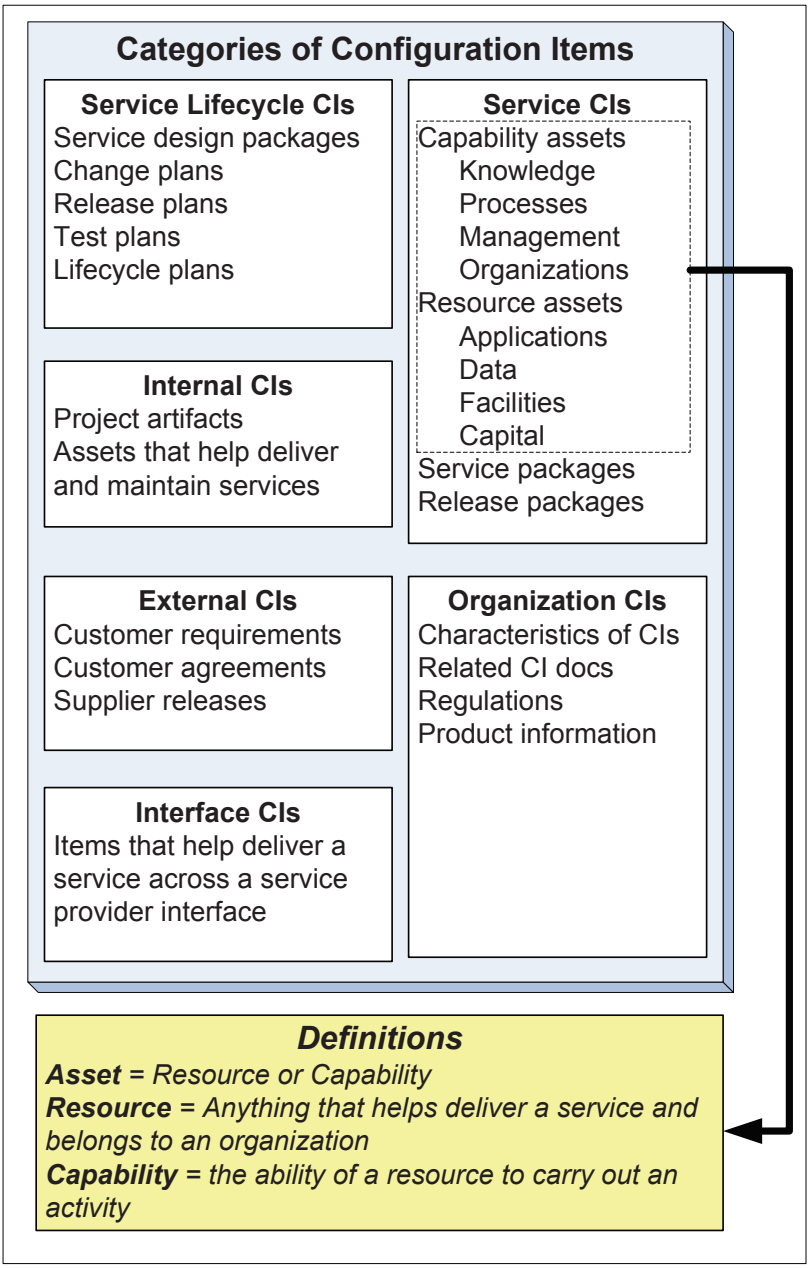
Stakeholder – Any party that has an interest in a service, configuration item, or other IT asset that may be subject to change.

Service Knowledge Management System



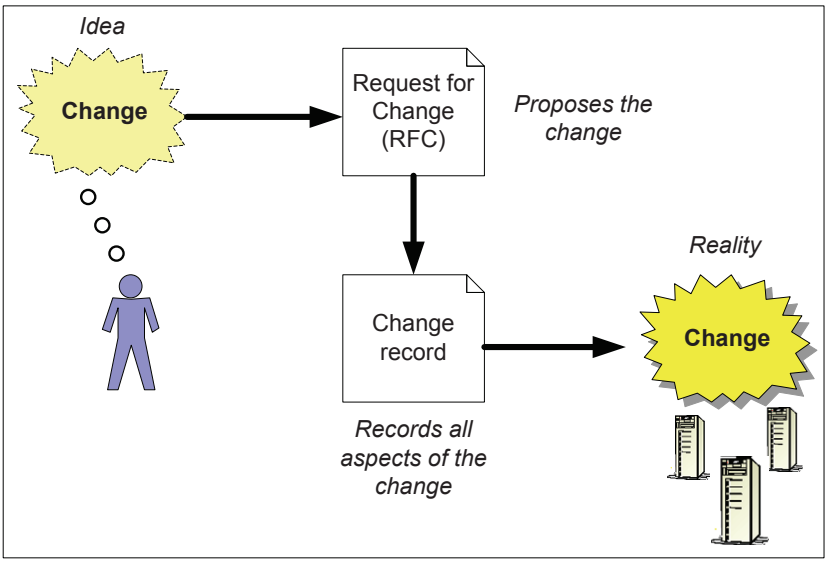
The service knowledge management system includes many Service Management Information Systems

Configuration Items (and Assets)



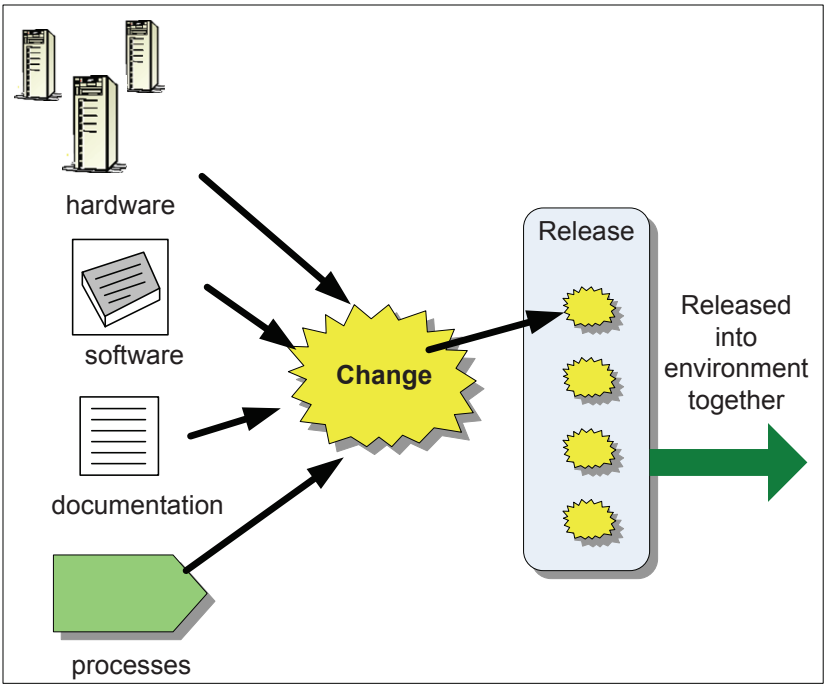
There are a variety of different types of CIs and assets

Change



Proposed changes are RFCs whereas change records record everything about proposed and implemented changes

Release



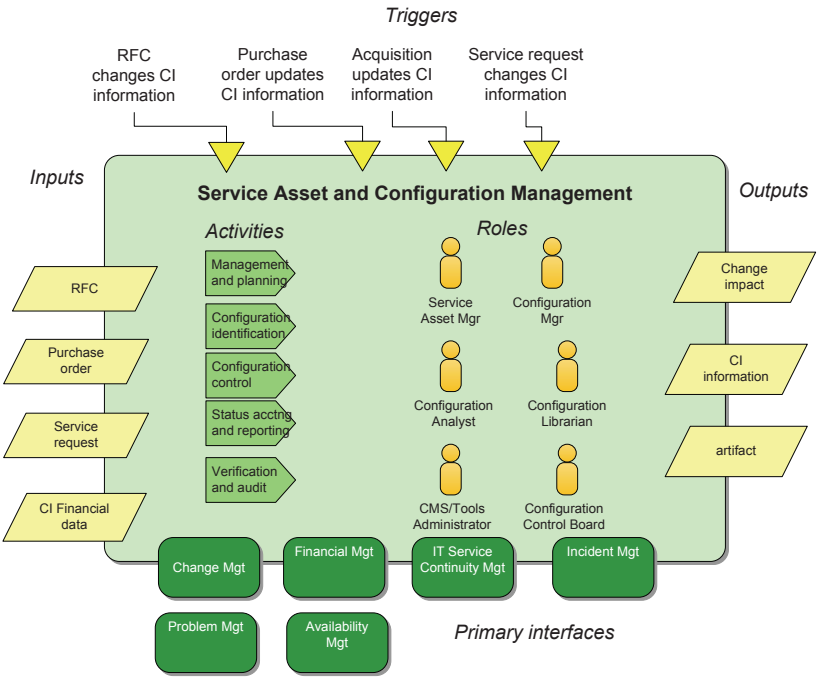
A release may include a number of changes

Service Asset and Configuration Management

Purpose

Control and track all CIs to promote integrity in the infrastructure.

Overview Diagram



Key Concepts

Asset – A capability or resource that is used in the delivery of a service. Also called service asset. There are many types of assets, including management assets, organization assets, process assets, knowledge assets, people assets, information

assets, application assets, infrastructure assets, and financial assets.

Asset Management – The process within Service Asset and Configuration Management (SACM) that deals with inventory of all service assets.

Configuration baseline – The configuration of a set of CIs that has been reviewed and agreed upon.

Configuration item – An element of the IT infrastructure that is managed as part of the delivery of an IT service, including people, hardware, software, services, facilities, SLAs, and documentation.

Configuration Management – The process within Service Asset and Configuration Management (SACM) that ensures that configuration items within the IT infrastructure are identified, information about the configuration items are maintained, and all updates are properly controlled.

Configuration management database (CMDB) – A virtual repository of information about configuration items.

Configuration Management System (CMS) – A system of databases and tools that manage information in multiple CMDBs, as well as additional information related to CIs.

Configuration model – A depiction of the relationships between CIs.

Definitive Media Library (DML) – The secure library that stores definitive versions of all electronic CIs.

Definitive spares – A secure store for CIs that are at the same levels at CIs in a test or live environment.

Secure library – A secure storage of electronic assets. This is a part of the CMS.

Secure store – A physical storage location storing IT assets. This is a part of the CMS.

Snapshot – The status of a set of configuration items at a point in time.

Roles

CMS/tools administrator – Administers and supports configuration management tools

Configuration Administrator/Librarian – Controls access to CI data

Configuration Analyst – Analyzes CI status and relationships

Configuration Control Board – Provides assessments in support of change authorization

Configuration Manager – Oversees configuration management activities and sets configuration management policies

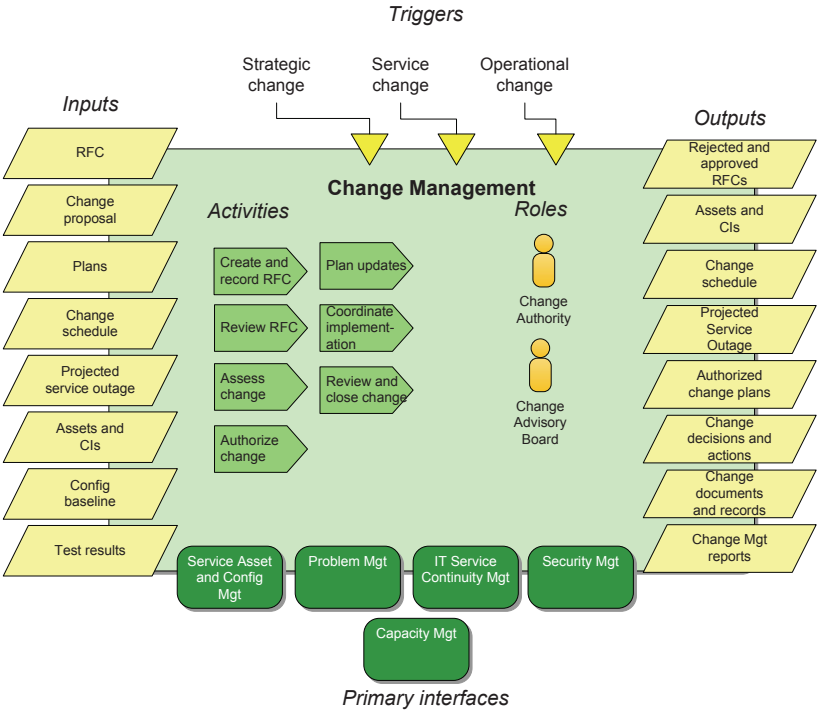
Service Asset Manager – Tracks service assets for financial and regulatory reasons

Change Management

Purpose

Manage all changes to the IT infrastructure in a controlled manner.

Overview Diagram



Key Concepts

Change assessment – An evaluation of the change request from various points of view.

Change authorization – Approval of a change request. There may be different authorization levels based on the type of change being considered.

Change priority – The order in which change request are considered for authorization.

Change process model – Predefined workflows for changes that fit within predetermined templates.

Change record – a record of a change throughout its lifecycle. The information in an RFC becomes the initial part of a change record.

Remediation – The approach or plan to be followed if a change is not successful. This may involve backing out an installation, invoking continuity plans, or some other approach.

Request For Change (RFC) – A record of a proposed change. Also called “change request”.

Risk categorization – An evaluation of the overall risk of a change request to the business.

Standard changes – A very low-risk change that is pre-authorized for implementation.

Roles

Change authority – Authorizes changes to be performed based on assessment information from various stakeholders

Change manager – Oversees the Change Management process

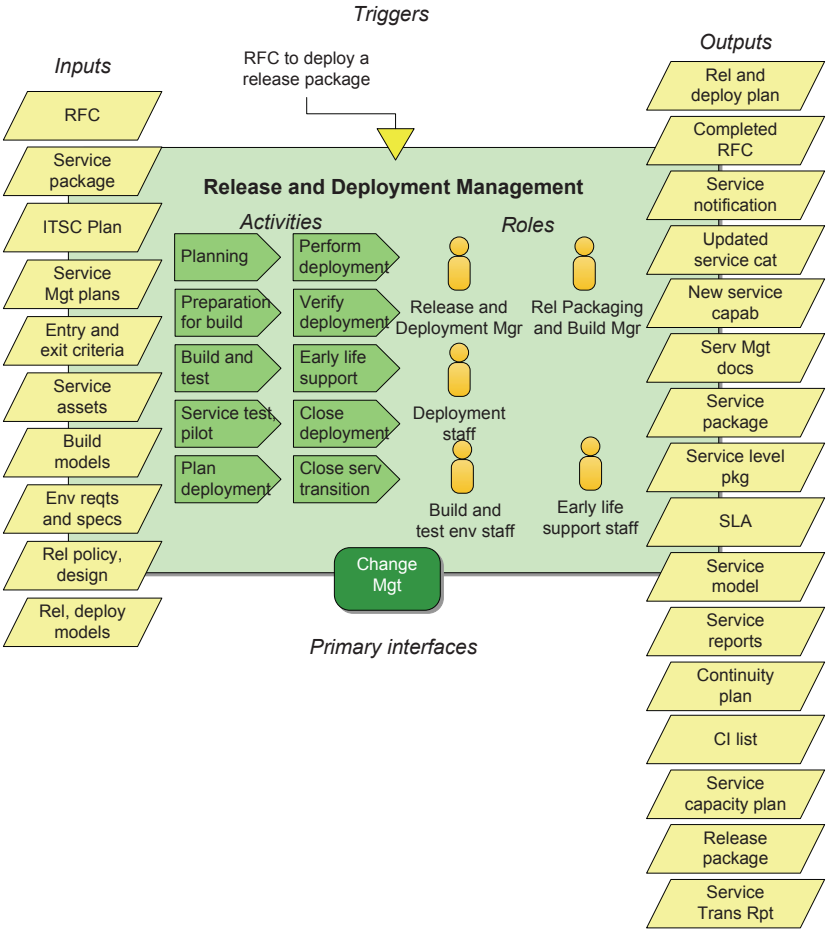
Change Advisory Board (CAB) – A provisional team organized to assess proposed changes and give advice to the change authority concerning the risk of implementing those changes

Release and Deployment Management

Purpose

Build, test, and deploy capabilities to provide services. This does not include application development.

Overview Diagram



Key Concepts

Early life support – A period of additional attention and support for an IT service immediately after deployment. This consists of more intensive monitoring, adjustment of service level targets, and additional resources to handle related incidents and problems.

Pilot – Deployment of an IT service or asset that is limited for trial purposes.

Release – A group of changes that are tested, packaged, and deployed into the IT infrastructure at the same time. These changes may include hardware, software, documentation, or other items. The package of items is sometimes referred to as a release package.

Release and deployment model – A standard or repeatable model for carrying out a release. There may be such models for different types of releases.

Service rehearsal – A type of service testing that involves performing as much of the service as possible before actual deployment.

Service retirement and cleanup – Services or service assets may be retired as part of a deployment action.

Service transfer – Deployment may involve transfer of service from one service provider to another.

Roles

Release and Deployment Manager – Oversees the Release and Deployment Management process

Release Packaging and Build Manager – Oversees the creation of release builds

Deployment staff – Distributes and installs releases

Early life support staff – Performs post-deployment tasks for a limited time to bring stability to newly-deployed services

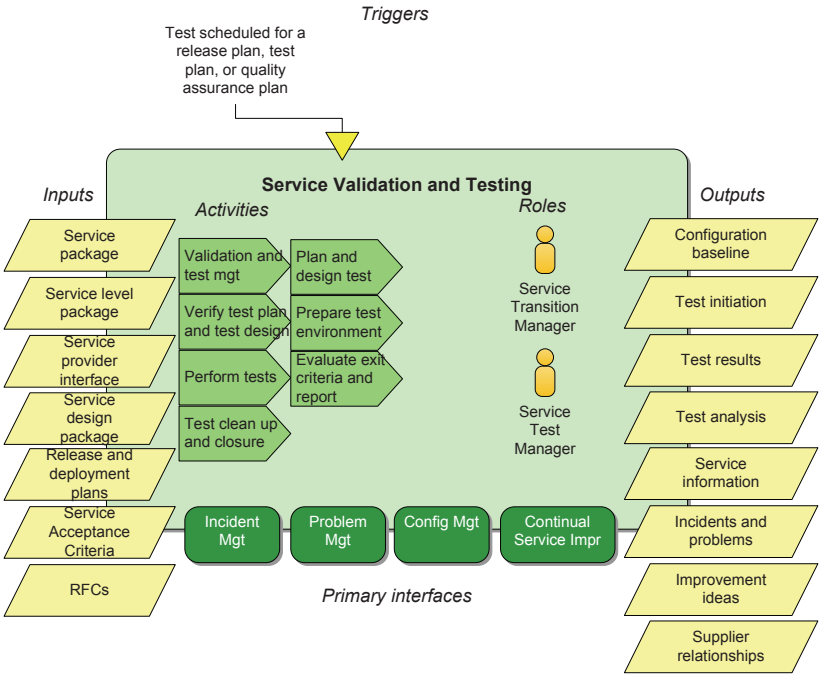
Build and test environment staff – Creates and tests the release builds

Service Validation and Testing

Purpose

Ensure that a new or changed service will meet customer requirements and will be fit for purpose and fit for use.

Overview Diagram



Key Concepts

Service Design Package – The documented requirements and design of a service.

Service level package – The level of utility and warranty that goes with a specific service package.

Service model – A depiction of service functionality.

Test model – A model of how to define each service deliverable.

Types of testing – Various aspects of what to test in a service, including usability, accessibility, performance, availability, compliance, remediation, etc.

Validation – the practice of identifying that a new or modified configuration item meets needs of the business.

Verification – the practice of identifying that a new or modified configuration item meets requirements.

Roles

Service Test Manager – Oversees and directs all service testing

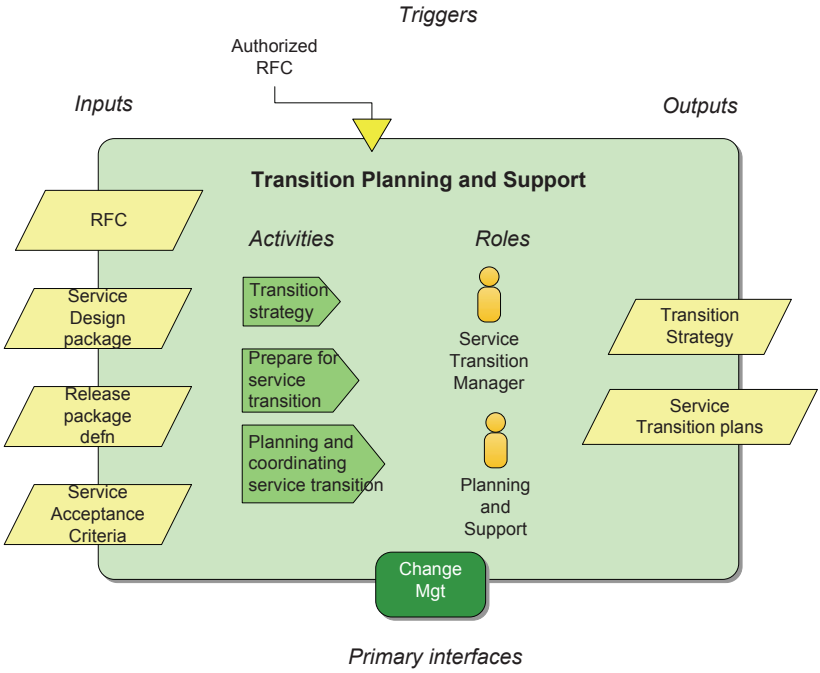
Test Support – Provides support for test activities, including maintenance of the test environment, creation of test cases, and providing the test reporting system

Transition Planning and Support

Purpose

Plan service transitions that appear in each stage of an IT service's lifecycle.

Overview Diagram



Key Concepts

Service Design Package – specifications, models, architectures, designs, plans, and acceptance criteria.

Service Transition – a stage in the lifecycle of an IT service.

Roles

Service Transition Manager – Oversees the progression of a service design package into an operational service

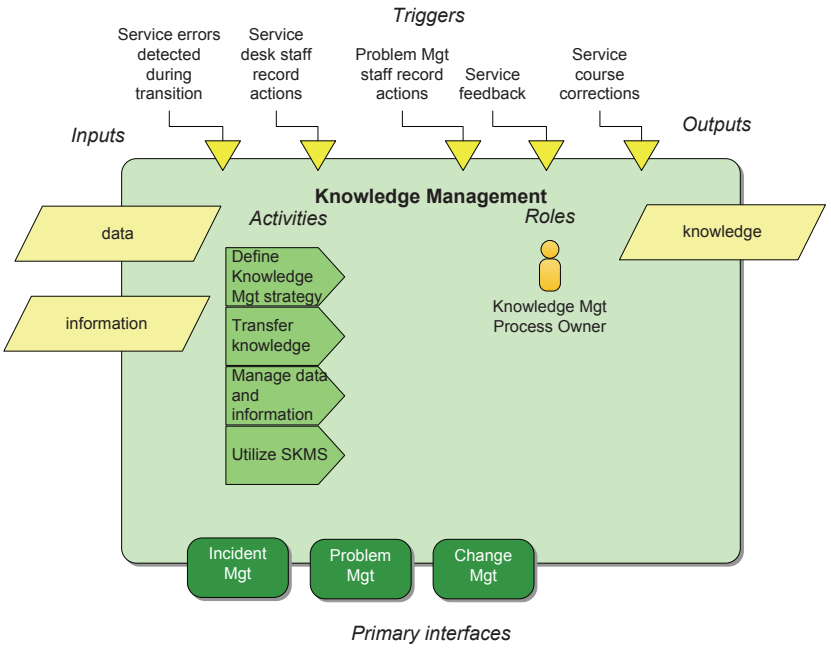
Planning and support – Provides more detailed tasks in support of the Service Transition Manager

Knowledge Management

Purpose

Ensure that the right information is provided to the right roles at the appropriate time.

Overview Diagram



Key Concepts

Data – disjointed facts about events.

Information – context for data.

Knowledge – Insights gained from individuals about events concerning how events happened.

Knowledge Management Strategy – Overall policies, governance, roles, and procedures for knowledge management.

Service Knowledge Management System – The overall system that encompasses all Service Management Information Systems, including

- Availability Management Information System
- Capacity Management Information System
- Configuration Management System
- Known Errors Database
- Security Management Information System
- Supplier and Contracts Database
- and others

Wisdom – Discernment concerning why events happened.

Roles

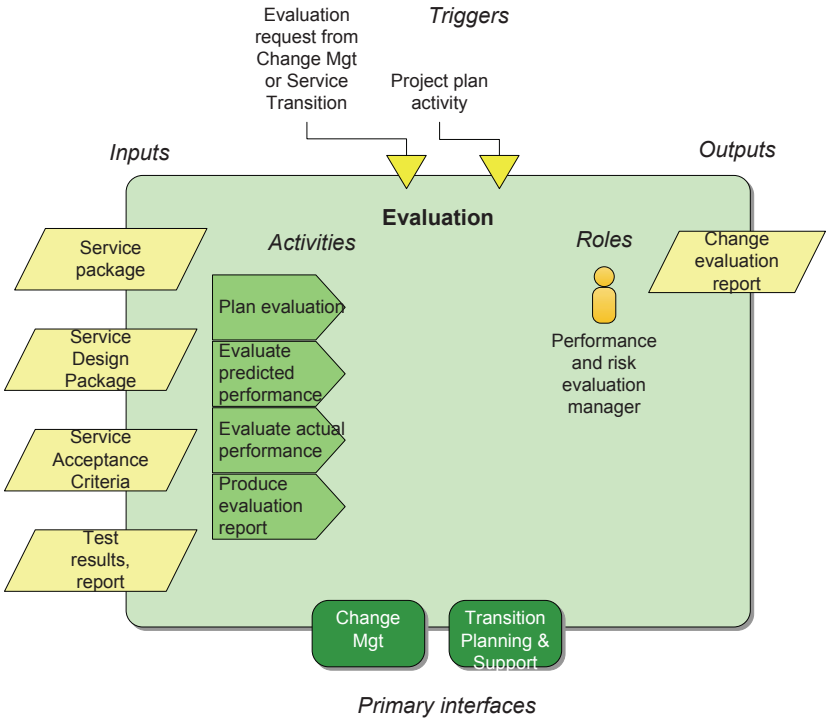
Knowledge Management Process Owner - Provides high-level direction for knowledge management and ensures that knowledge management is implemented and performed to support business objectives

Evaluation

Purpose

Determine the ramification of a proposed service change whether as a result of a Request for Change, a new Service Design Package, or testing.

Overview Diagram



Key Concepts

Actual performance – A measure or assessment of the past effects of an implemented change.

Deviation – The determination that actual performance is acceptable.

Predicted performance – A measure or assessment of the effects of a future change.

Risk – A potential occurrence that may cause loss.

Risk management formula – Likelihood X impact.

Unintended effects – Side effects of a change, arrived at by discussions with stakeholders to determine effects other than those anticipated by the change request.

Roles

Performance and Risk Evaluation Manager – Identifies issues and risks as input to service testing and service transition

Other Practices

Communications and Commitment Management – The practice of providing effective communication to all affected parties concerning a change.

Organizational and Stakeholder Change Management – The practice of managing process and cultural changes among IT stakeholders. Many changes affect important underpinnings of how an organization works. This practice goes beyond mere deployment of changes to determine how to improve the acceptance of significant changes within an organization.

Stakeholder Management – The practice of resolving the needs and concerns of stakeholders of IT services. Stakeholders may represent a variety of interests, including customers, users, regulatory organizations, business units, partners, and others.

Additional Service Transition Roles

Process Owner – Provides high-level direction for a process and ensures that a process is implemented and performed to support business objectives

Service Owner – Provides high-level responsibility for the design, development, maintenance, and support of a service

Service Operation

Brief Description

In the Service Operation stage, a service is available for IT end users. During execution of the service, it is monitored to determine service levels as well as to look for operational faults.

Operational faults may be detected as events from service monitoring. Those events may be resolved within Event Management or may be escalated to Incident Management to be resolved by Service Desk personnel. In either case, the event is recorded as an incident and the service is restored as quickly as possible via either a workaround or some other resolution.

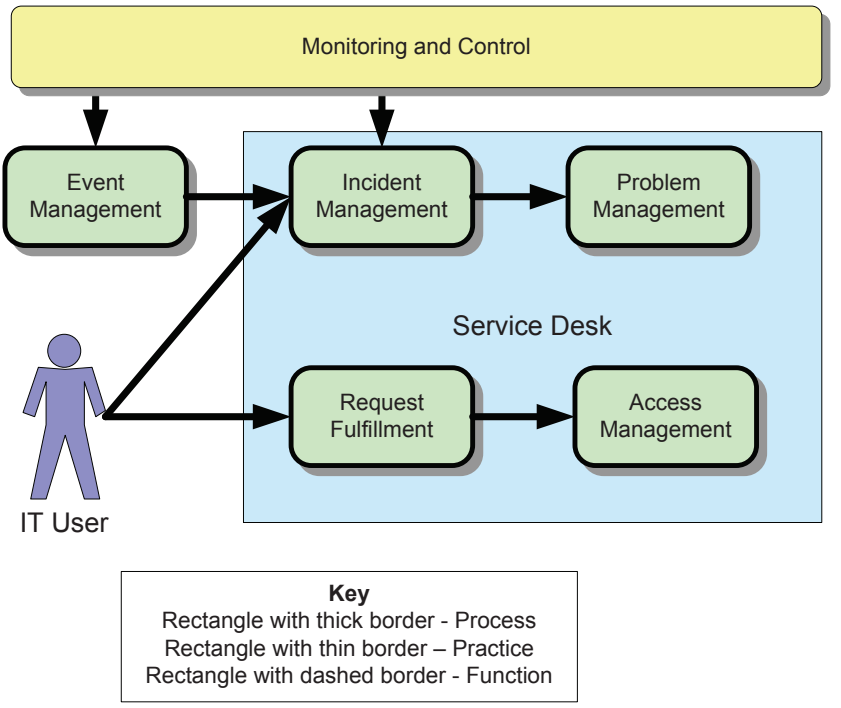
Faults may also be detected by users, who may contact the Service Desk to log an incident. The Incident Management process is used by the Service Desk to get the service restored to the user as quickly as possible.

The Problem Management process supports the Incident Management process by looking for incident trends (problems) and resolving root causes of those problems. This process also proactively addresses any faults not yet previously identified.

The user may also contact the Service Desk to carry out simple, virtually risk-free actions (service requests) that cannot be performed by the user (Request Fulfillment) or to provide access to services or service assets (Access Management).

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_5,
© Springer Science+Business Media, LLC 2008

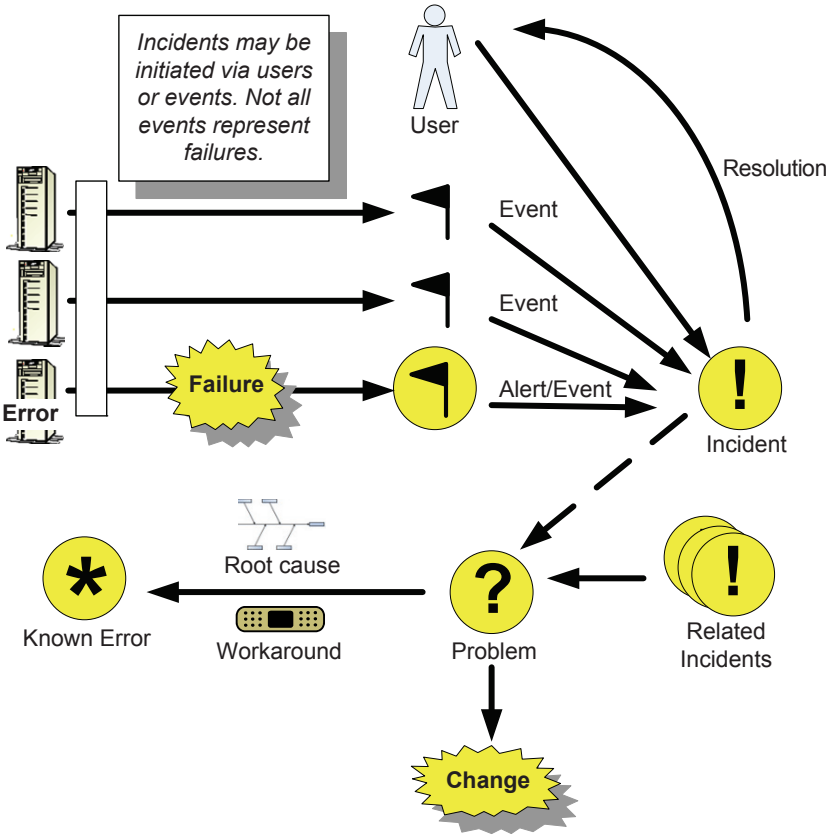
Overview Diagram



The service desk is at the heart of the service operation stage

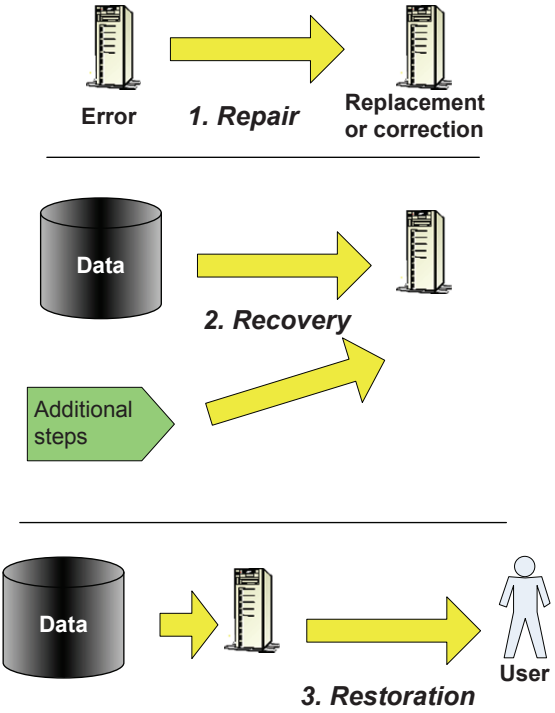
Service Operation Key Concepts

Events, Incidents, and Problems



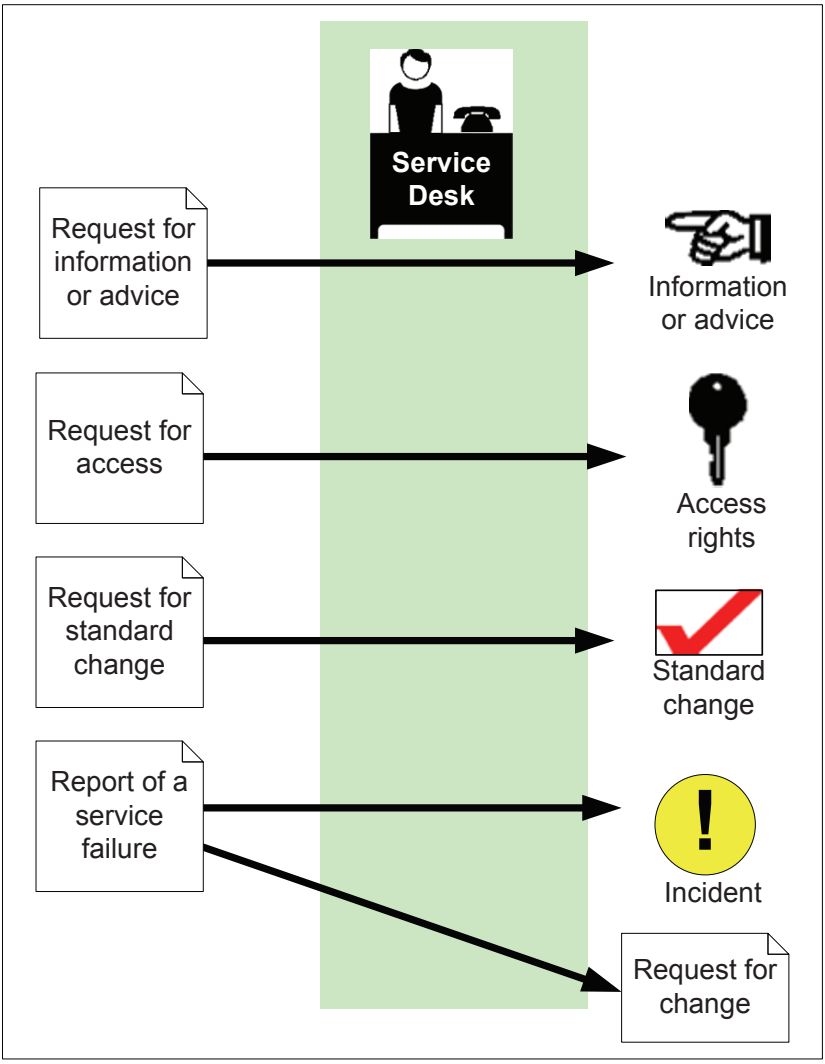
Events may turn into incidents, and related incidents may constitute a problem

Restoring a Service



After a service has been interrupted, it should be repaired, recovered, and restored

Service Desk



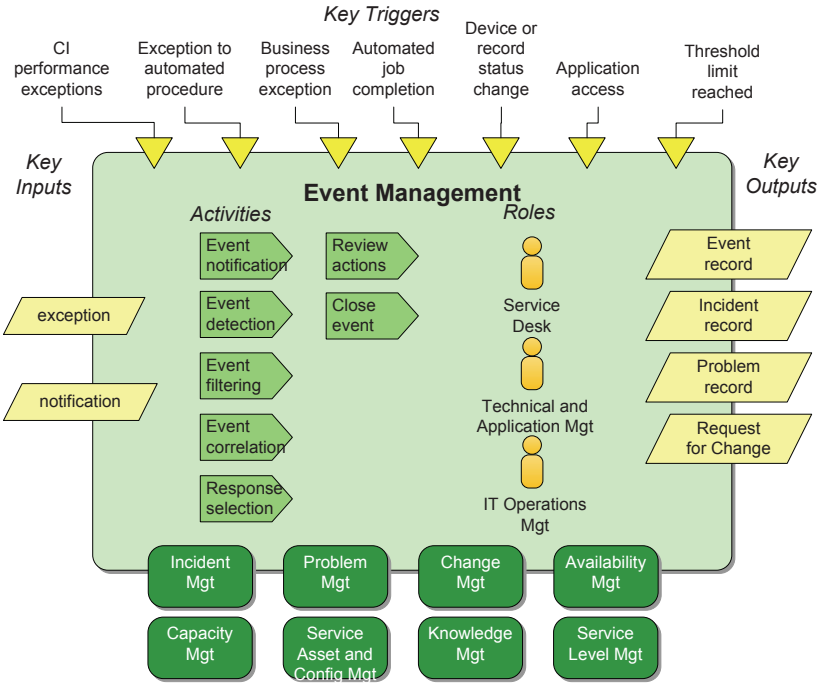
A user may submit a variety of things to the service desk which are then processed or routed to the appropriate team

Event Management

Purpose

To identify and resolve system events that represent failures within configuration items.

Overview Diagram



Key interfaces

Key Concepts

Event Correlation – Various system monitoring tools generate events according to predefined event generation rules. The usefulness of event management is closely tied to how well these rules are defined. Tightly constrained rules will not

generate enough events to identify many failures, whereas loosely constrained rules will generate many false positives.

Event response – Some events may have an automatic response associated with the event, such as restarting a process. Other events may require manual intervention, such as incident management or creation of an RFC.

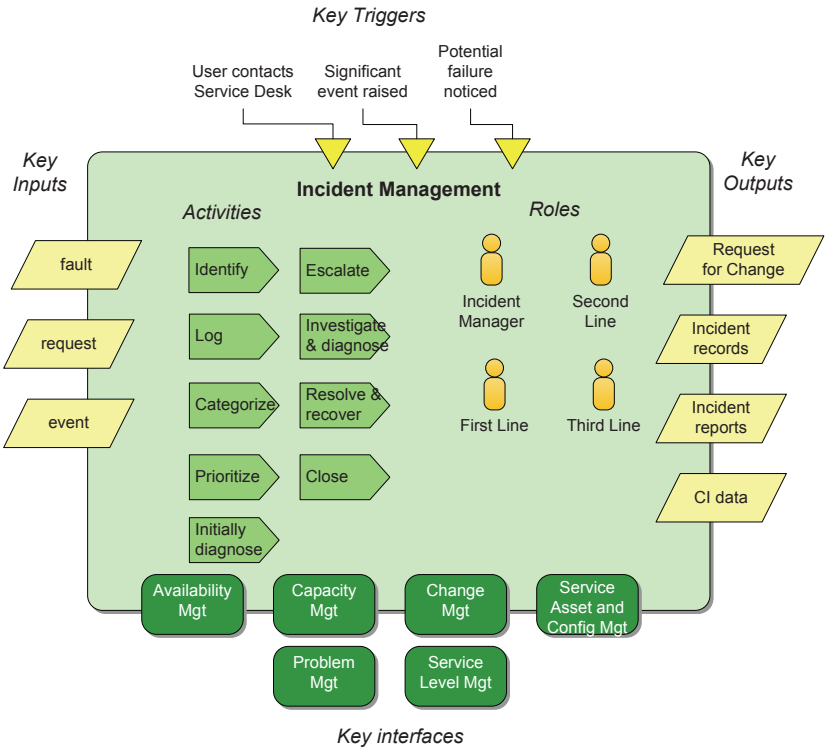
Monitoring – Monitoring is different from event management. Monitoring determines the status of a configuration item or service, whereas event management identifies changes in status of those CIs and services that represent faults within the IT infrastructure.

Incident Management

Purpose

To restore service operation to a user as rapidly as possible.

Overview Diagram



Key Concepts

Classification – Grouping similar types of incidents into categories.

Escalation – Incidents that cannot be resolved by available resources are escalated either to those with greater skills

(functional escalation) or to those who are at higher levels of management (hierarchical escalation).

Incident models – Similar types of incidents may follow similar paths to resolution. For this reason, predefined workflows for specific types of incidents may be created.

Major incidents – Some incidents are of such magnitude that they are treated individually. Such an incident may be treated as an individual problem in Problem Management.

Prioritization – The relative impact and urgency of an incident, where impact is the effect the incident has on the business, and urgency is how long it will take for the incident to have that effect.

Recovery – Returning a configuration item to its working state after resolution.

Repair – Replacing or fixing a configuration item.

Resolution – Addressing the root cause of an incident or problem via a repair or a workaround.

Timescales – A time period in which an incident should be resolved or escalated. Because incident management is focused on rapid restoration of services, timescales are important.

Roles

Incident Manager – Oversees the incident management process and incident management staff

First line – Provides initial handling of user contacts with the service desk

Second line – Provides more technical expertise for resolving incidents

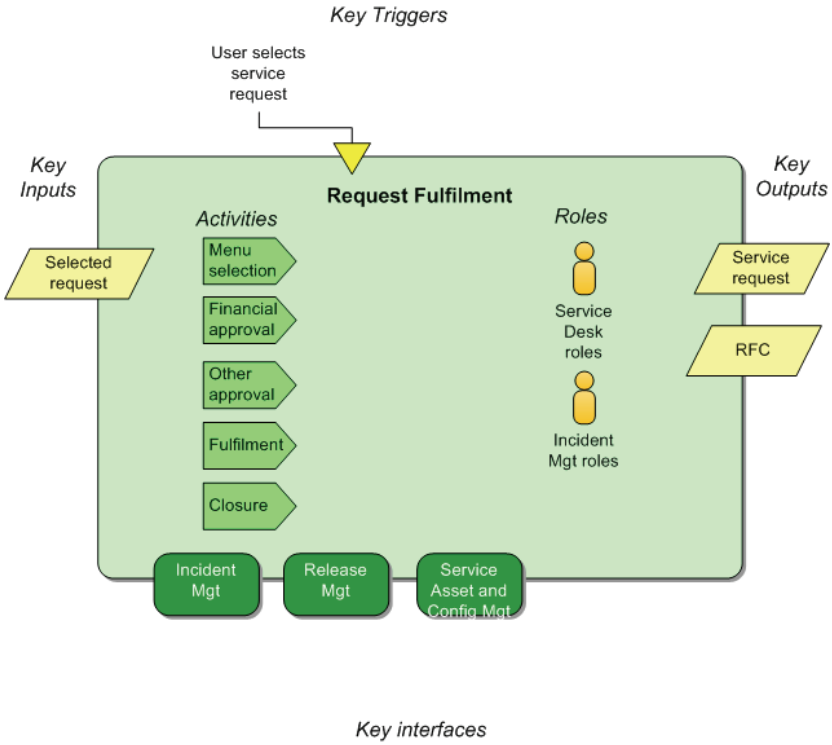
Third line – Provides the most in-depth technical expertise in support of incidents

Request Fulfillment

Purpose

Request fulfillment processes service requests and requests for information. Access-related service requests are processed by Access Management.

Overview Diagram



Key Concepts

Request Model – a predefined workflow for handling a specific type of service request.

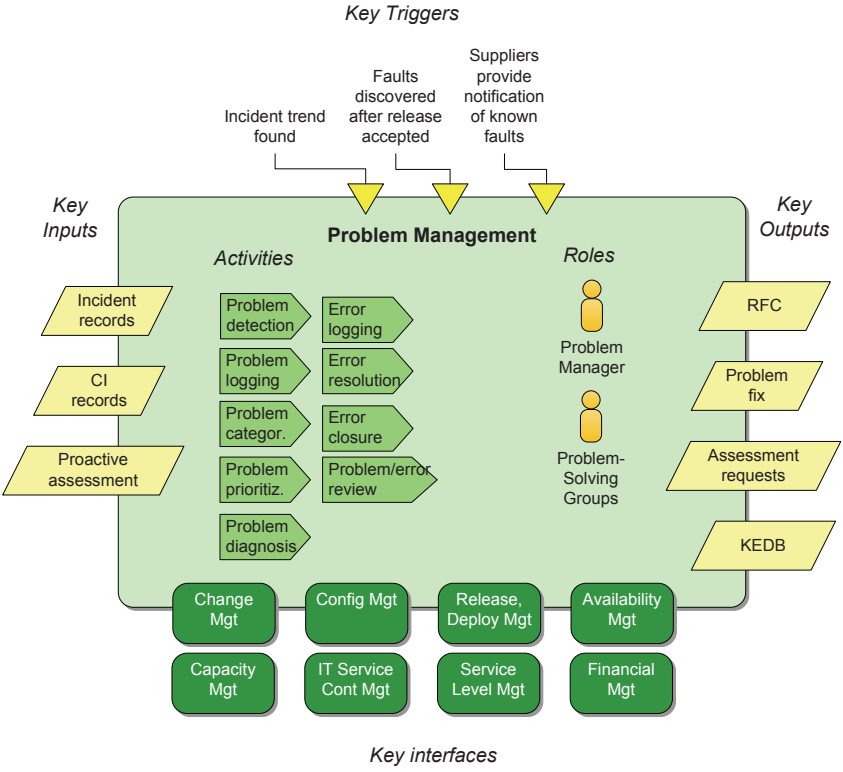
Service Request – a standard (preapproved) change that is straightforward and virtually risk-free.

Problem Management

Purpose

To diagnose root causes of incidents, request changes that will resolve those root causes, and reduce the number of future incidents.

Overview Diagram



Key Concepts

Known Error – a problem for which the root cause has been determined and a workaround or resolution has been created.

Proactive problem management – looking for potential problems before they are reported by other processes or functions and resolving those problems.

Problem – a problem is a root cause of a group of related incidents.

Problem Model – a predefined workflow for handling a specific type of problem.

Reactive problem management – resolving problems that have already been uncovered by incident management or some other source.

Roles

Problem Manager – Focal point for problem management activities and coordinator of teams resolving problems

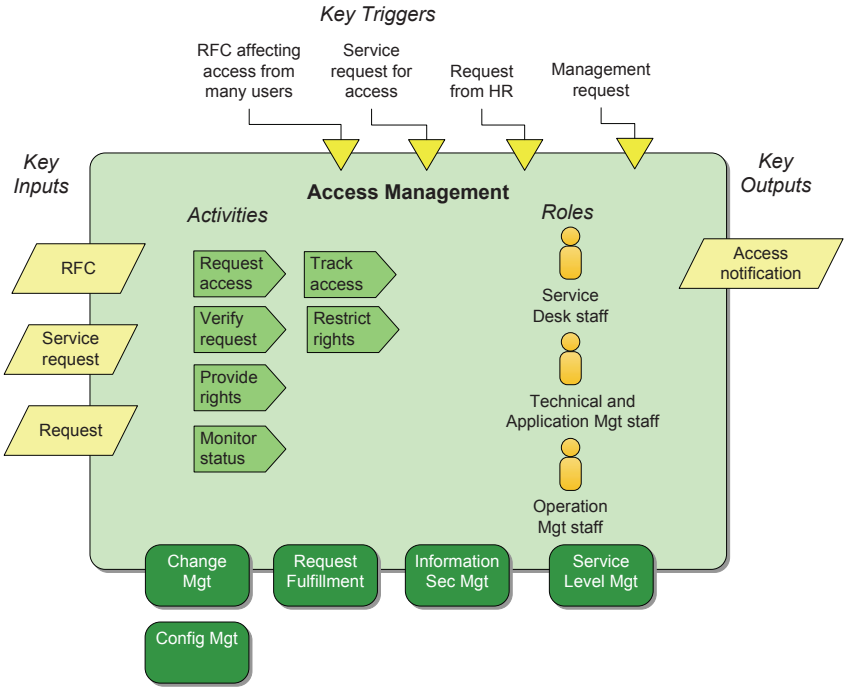
Problem-Solving Groups – Teams representing various technical groups provisionally assigned to resolve problems

Access Management

Purpose

To provide rights for a user to access a service.

Overview Diagram



Key Concepts

Access – the ability to make use of a specific configuration item. There may be different types of access, such as read, write, execute, etc.

Directory services – An application that records the rights given to each identity and allows modifications to those rights.

Identity – the name of a user or group. Access rights are granted to identities.

Rights – permission given to an identity.

Other Practices

Facilities and Data Center Management – Management of the physical location where IT resources are housed. This location is often referred to as a data center.

Information Security Management and Service Operation – Enforcement of information security policy during service operations.

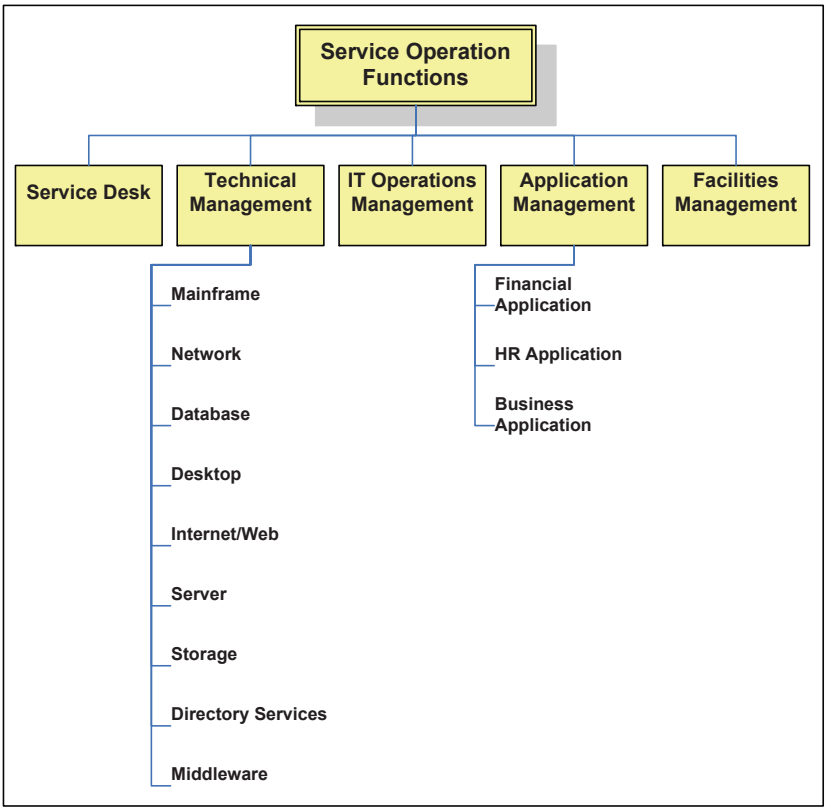
IT Operations – The operation and management of specific types of technology resources. Support for these resources requires specific types of expertise. Examples include the following:

- Mainframe Management
- Server Management and Support
- Network Management
- Storage and Archive
- Database Administration
- Directory Services Management
- Desktop Support
- Middleware Management
- Internet/Web Management

Monitoring and Control – The cycle of service monitoring and response.

Service Operation Functions

A “function” is an abstract organizational unit within an IT organization. It represents a real organization or group, but not a process. A function may use one or more IT processes or practices to carry out its objectives. There are 5 primary functions within Service Operation, some, of which, are divided into smaller functions.



Service operation functions

Application Management – Control of the entire lifecycle of an application

Facilities Management – Management of IT data centers and other physical IT facilities

IT Operations Management – Ongoing operation and execution of IT services and IT resources in support of those services

Service Desk – User support for IT services

Technical Management – Provides specialized technical skills to carry out IT operations

Additional Service Operation Roles

Application Management Roles

Application Manager/Team Leader – Oversees application support staff

Application Analyst/Architect – Provides technical support of deployed applications

IT Operations Management Roles

IT Operations Manager – Oversees control of IT operations and facilities

Shift Leaders – Supervises IT operations staff for a specific shift

IT Operations Analysts – Experience operators who provide more detailed planning and analysis in support of operations

IT Operators – Performs daily operational tasks

Service Desk Roles

Service Desk Manager – Oversees all service desk activities and supervisors

Service Desk Supervisor – Oversees service desk activities for a specific shift

Service Desk Analyst – Provides first-level support for incidents and service requests

Super User – Users who act as liaison between the service desk and the user community

Technical Management Roles

Technical Manager/Team Leader – Provides leadership for a technical team

Technical Analyst/Architect – Determine stakeholder needs for a technical domain and provides analysis in support of that technical domain

Technical Operator – Performs daily technical operations tasks

Continual Service Improvement

Brief Description

During the Continual Service Improvement stage, the IT organization collects data and feedback from users, customers, stakeholders, and other sources to enhance services and how they are provided.

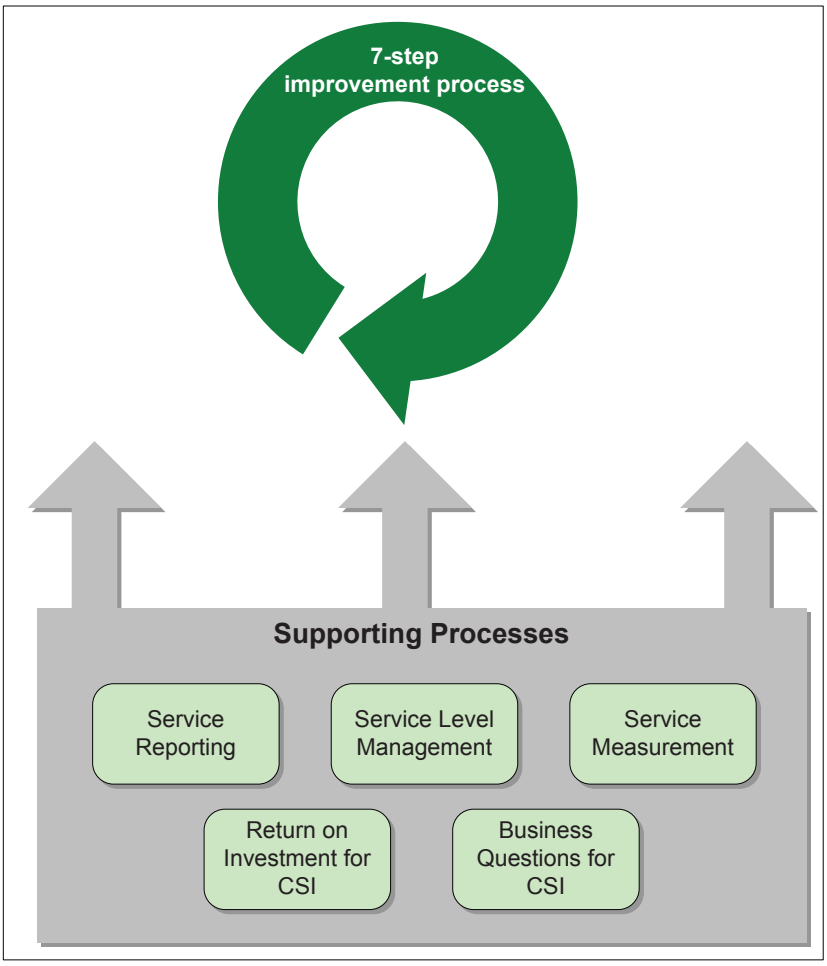
This involves the use of a 7-step improvement process that collects data, analyzes the data, provides recommendations, and implements those recommendations.

In support of the improvement process, Service Level Management collects information from IT users and customers and data from the operation of the services. Service measurement and reporting provides standard vehicles for describing the performance of the services.

Finally, all service improvements must be scrutinized according to whether they meet the needs of the business and provide an overall return on investment.

J.O. Long, *ITIL® Version 3 At a Glance*, DOI: 10.1007/978-0-387-77393-3_6,
© Springer Science+Business Media, LLC 2008

Overview Diagram



A variety of ongoing processes support the Continual Service Improvement lifecycle stage

Practices

7-Step Improvement Process – A generic process for improvement based on measurement, analysis, and corrective action. This can be used to continuously improve service management.

Business Questions for CSI – The practice of engaging IT management with business management in order to satisfy business goals using IT services.

Return on Investment for CSI – The establishment of a business case for IT service management based on measuring and reporting return on investment.

Service Measurement – Providing accurate and consistent measurements of service availability, reliability, and performance.

Service Reporting – The practice of reporting on service achievements, trends, and improvements.

Roles

CSI Manager – Oversees all continual service improvement activities

Process Owner – Champions a process and oversees its management and execution

Reporting Analyst – Reports on service achievements and trends

Service Knowledge Management – Oversees knowledge management for the enterprise

Service Manager – Has overall responsibility for development, evaluation, and maintenance of IT services

Service Owner – Owns a specific service, although supporting components and resources may be managed elsewhere

Index