ITIL Foundation

ITIL Foundation Certification

itSM Solutions®
IT Experience. Practical Solutions.

Acknowledgements

COPYRIGHT

Publisher – itSM Solutions Publishing, LLC. 31 S. Talbert Blvd. #295. Lexington, NC 27292 USA

Phone: +1 336.243.4876, Fax +1 336.499.1172

Part Number: itSM004 Rel. 1.6

Find us on the web at http://www.itsmsolutions.com.

Authors: David Nichols & Janet Kuhn

NOTICE OF LIABILITY – This publication is distributed "As Is," without warranty of any kind, either expressed or implied, respecting the content of this publication, including but not limited to implied warranties for the publications quality, performance, merchantability, or fitness for any particular purpose. Neither the authors, nor itSM Solutions LLC, its dealers or distributors shall be liable with respect to any liability, loss or damage caused or alleged to have been cause directly or indirectly by the contents of this guide.

DOCUMENT INFORMATION

Type - ITIL Certification Course

Program - ITIL Foundation

Contents

Chapter 4:

Service Operation

Objectives

- Account for main goals & objectives of Service Operation.
- Briefly explain what value Service Operation provides to the business.
- Explain the high-level objectives, basic concepts, process activities and relationships for Incident Management & Problem Management.
- State the objectives and basic concepts for Event Management, Request Fulfillment & Access Management.
- Explain the role, objectives & organizational structures for the Service Desk function.
- State the role, objectives & organizational overlap of the Technical Management function, Application Management function & IT Operations Management function.

Terms-to-Know

Alert – A warning that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed

Event – A change of state that has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an alert or notification created by any IT Service, Configuration Item or monitoring tool.

Impact – A measure of the effect of an incident, problem or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.

Incident – An unplanned interruption to an IT Service or reduction in the quality of an IT Service. Failure of a Configuration Item that has not yet affected a IT Services is also considered an Incident.

IT Operations Control – The function responsible for monitoring and Control of the IT Services and IT Infrastructure.

Known Error – A Problem that has a documented root cause and a workaround. Known Errors are created and managed throughout their lifecycle by Problem Management. Known Errors may also be identified by development or Suppliers.

Known Error Database – A database containing all Known Error records. This database is created by Problem Management and used by Incident and Problem Management. The known Error Database is part of the Service Knowledge Management system.

Operations Bridge – A physical location where IT Service and IT infrastructure are monitored and managed.

Priority – A Category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority 2 incidents must be resolved within 12 hours.

Problem – A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.

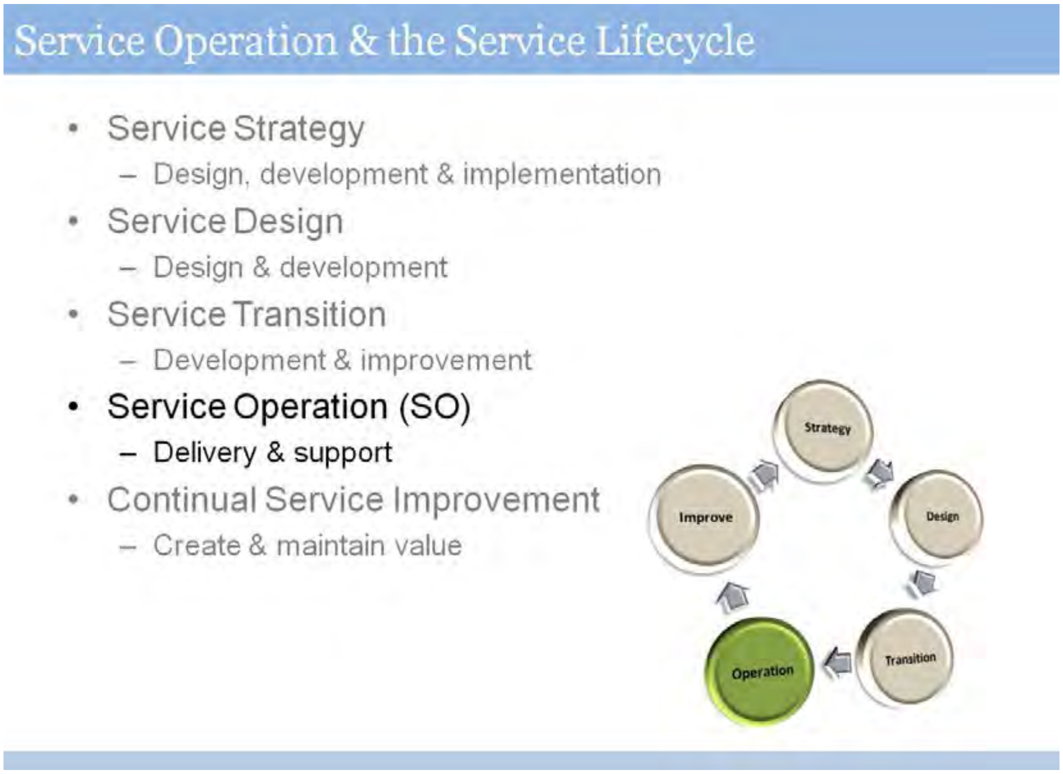
Service Request – A request from a user for information, advice, a standard change, or access to an IT Service. Service Requests are usually handled by a Service Desk and do not require a Request for Change (RFC) to be submitted.

Urgency – A measure of how long it will be until an incident, problem or change has a significant impact on the business. For example a high-impact Incident may have low Urgency if it will not affect the business until the end of the financial year. Impact and Urgency are used to assign priority.

Workaround – Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available; for example by restarting a failed Configuration Item. Workarounds for problems are documented in Known Error Records, and workarounds for incidents without associated Problem Records are documented in the Incident Record.

Lesson 9

Introduction to Service Operation

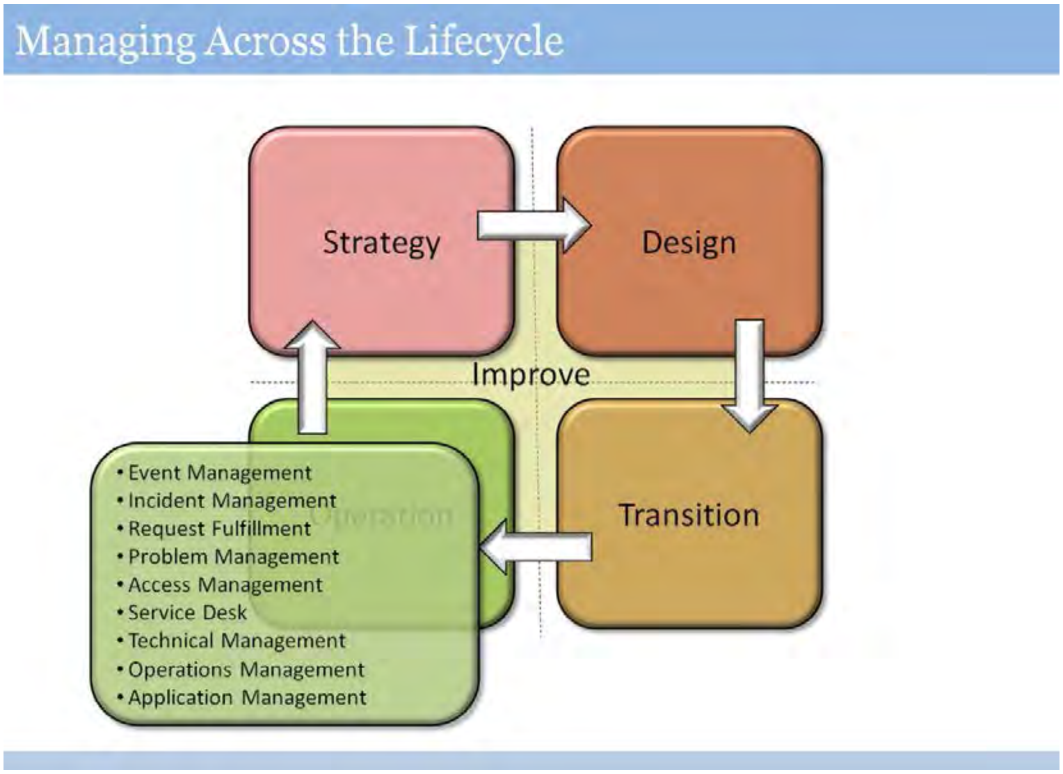


Service Operation & the Service Lifecycle

- Service Strategy
  - Design, development & implementation
- Service Design
  - Design & development
- Service Transition
  - Development & improvement
- Service Operation (SO)
  - Delivery & support
- Continual Service Improvement
  - Create & maintain value

Service Operation & the Service Lifecycle

Service Operation coordinates the processes and activities for delivering and managing services at their agreed levels. It is where most of the business community comes in contact with IT because Service Operation "makes IT services happen" in the eyes of the customer.



Managing Across the Lifecycle

Strategy

Design

Improve

Transition

Operation

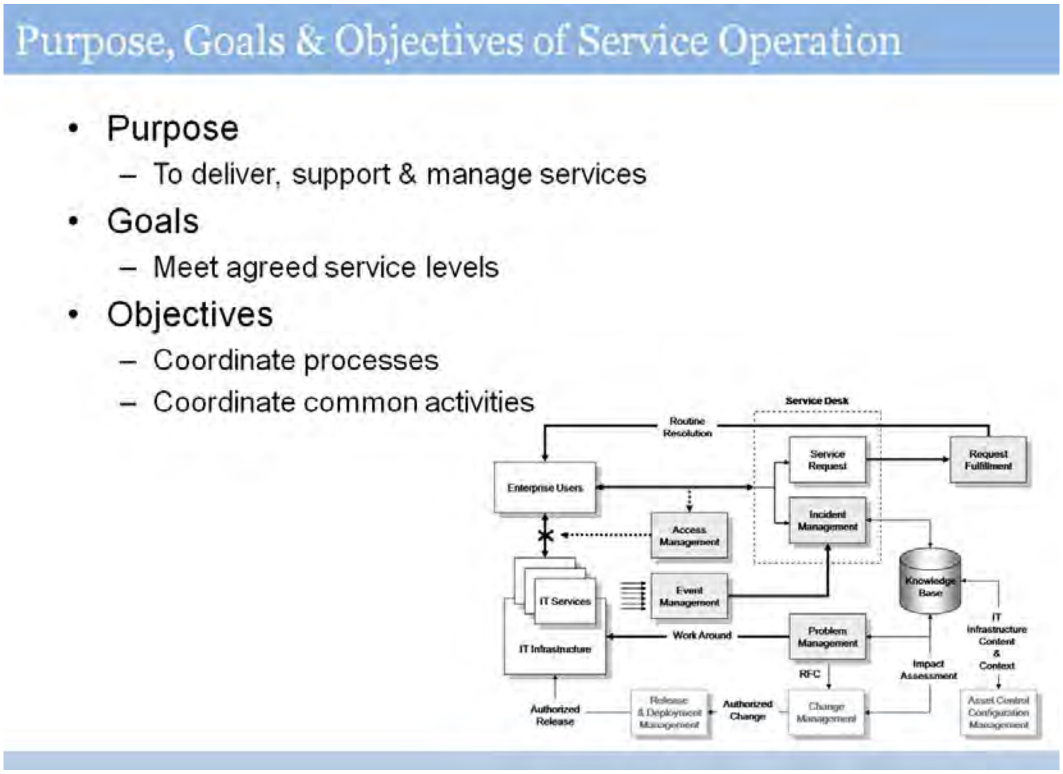
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management
- Service Desk
- Technical Management
- Operations Management
- Application Management

Managing Across the Lifecycle

Service Operation delivers and supports IT services. It directly touches the business side of the organization, and, thus, represents the face of IT to the majority of the user community.

Although Service Operation executes the actual operation of services as prioritized by Service Strategy, designed by Service Design, and transitioned by Service Transition, its responsibilities extend far beyond the technical side of IT Operations.

It provides inputs to the Continual Service Improvement phase (CSI) on how to improve services, as well as their accompanying support and delivery processes. It also actively participates in the Strategy, Design and Transition processes as both consultant and hands-on practitioner.



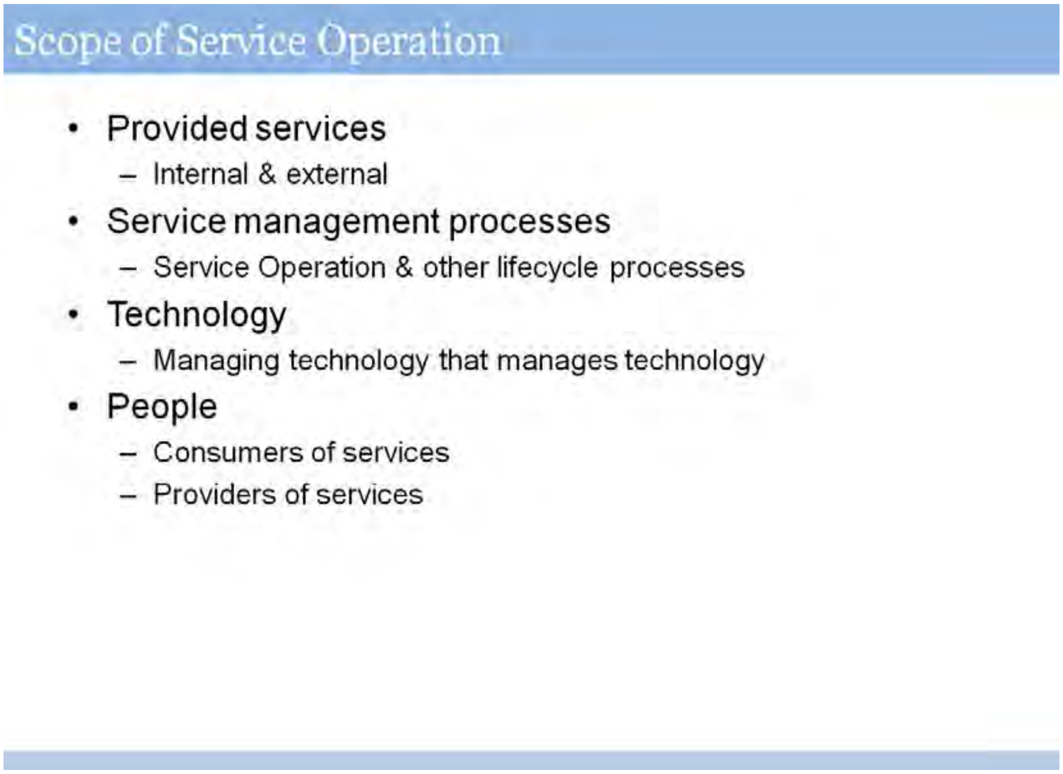
Purpose, Goals & Objectives of Service Operation

- Purpose
  - To deliver, support & manage services
- Goals
  - Meet agreed service levels
- Objectives
  - Coordinate processes
  - Coordinate common activities

Purpose, Goals & Objectives of Service Operation

The delivery and support of an IT service requires a tremendous amount of coordination of resources (people, technology, processes and functions). This effort provides the IT service at the agreed level of service within the defined resource constraints.

On a day-by-day basis, Service Operation manages the technology under its purview and continually monitors its services and technology to ensure that it is meeting the agreed objectives. Service Operation also continually seeks ways to improve its performance..



Scope of Service Operation

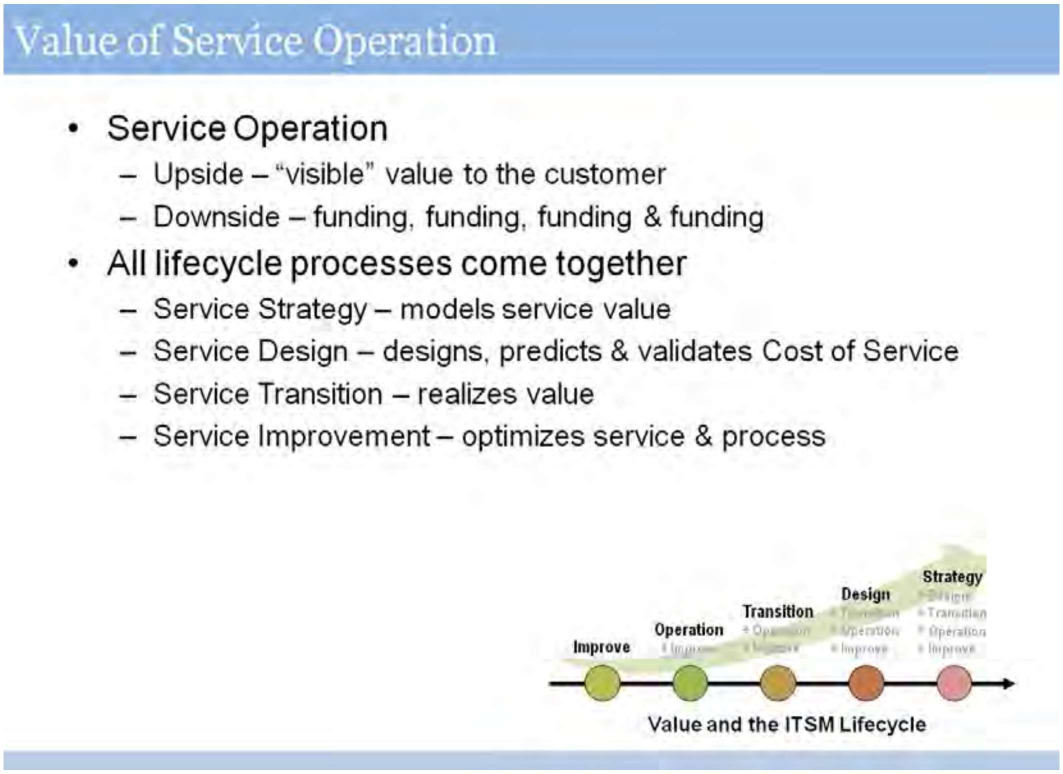
- Provided services
  - Internal & external
- Service management processes
  - Service Operation & other lifecycle processes
- Technology
  - Managing technology that manages technology
- People
  - Consumers of services
  - Providers of services

Scope of Service Operation

Service Operation's scope extends over all of the services provided by IT in support of business processes. This includes services provided by internal staff, as well as those provided by external service providers. Its scope also includes various touch points within the other Service Lifecycle domains such as Continual Service Improvement, Service Transition, Service Design, and Service Strategy.

The functions and processes of Service Operation involve highly complex tasks associated with managing its technology.This requires that all of the technology that supports or manages the IT infrastructure thoroughly integrate into the support processes to enable efficient and effective delivery of IT services.

Similarly, supporting today’s complex technological infrastructures demands that IT become a service provider within a multi-provider environment. Many of today’s services consist of both internally and externally provided services. However, from the customer’s viewpoint, it all "belongs" to the internal IT organization.



Value of Service Operation

- Service Operation
  - Upside – "visible" value to the customer
  - Downside – funding, funding, funding & funding
- All lifecycle processes come together
  - Service Strategy – models service value
  - Service Design – designs, predicts & validates Cost of Service
  - Service Transition – realizes value
  - Service Improvement – optimizes service & process

Improve
Operation
+ Improve
Transition
+ Operation
+ Improve
Design
+ Transition
+ Operation
+ Improve
Strategy
+ Design
+ Transition
+ Operation
+ Improve

Value and the ITSM Lifecycle

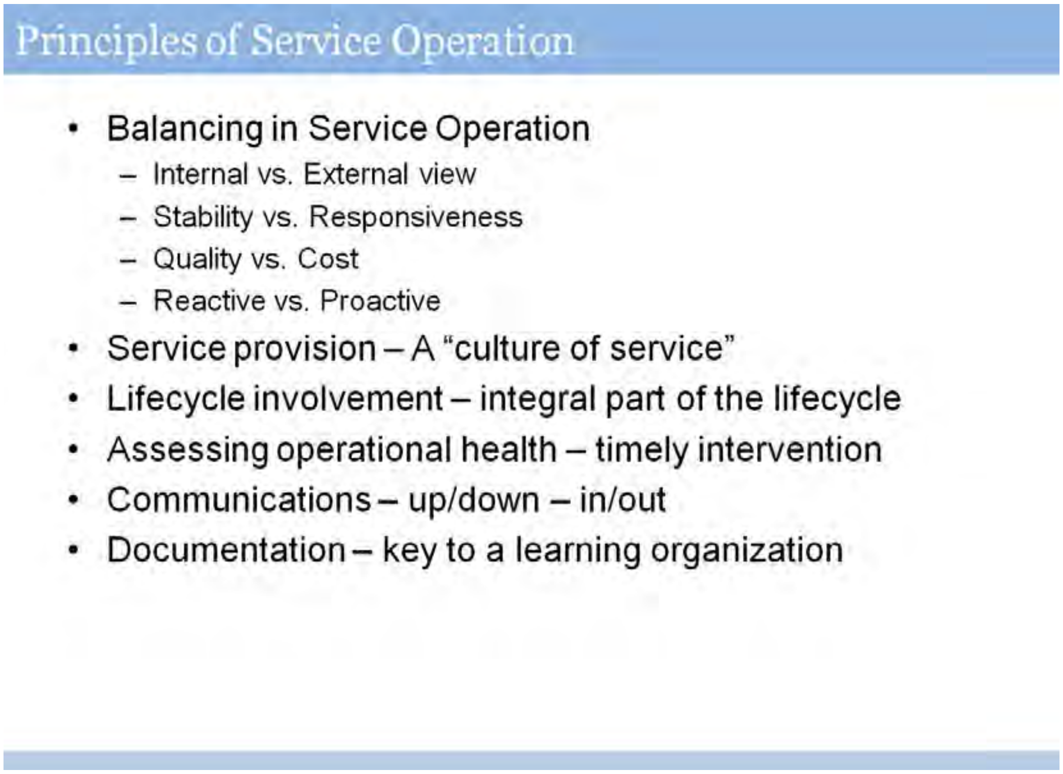
Value of Service Operation

Service Operation brings together the outcomes of all of the phases of the IT Service Lifecycle. Service Strategy models the IT service, Service Design validates it, Service Transition builds it and moves it into operation, and Continual Service Improvement optimizes it.

Up to this point in the IT Service Lifecycle, all of these efforts are transparent to the vast majority of the business customers and user community. However, Service Operation is "where the rubber hits the road." It is the face or visible part of IT that the average business person comes into contact with most often

If there is an upside to Service Operation, it is that the business customers form much of their perception of IT and the services it provides through their interactions with the functions and processes of Service Operation.

If there is a downside to Service Operation, it is that the activities become part of the landscape. It becomes difficult to justify necessary resources to support aging deficient services, support staff and tools, or make an IT service better.



Principles of Service Operation

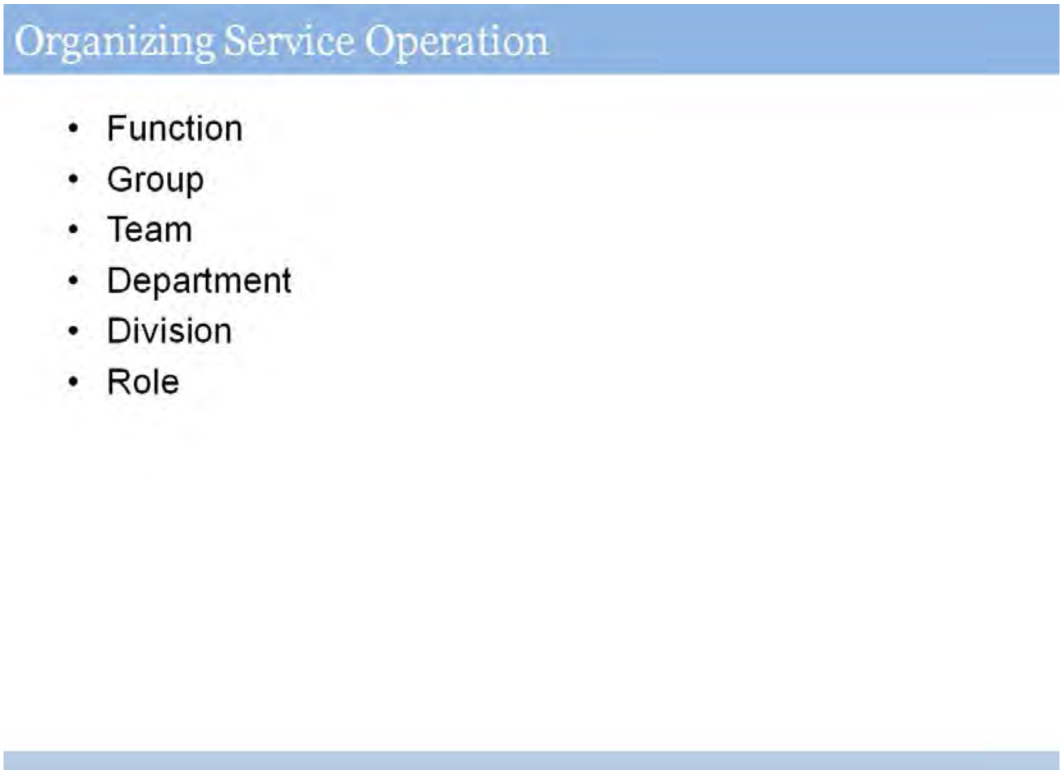
- Balancing in Service Operation
  - Internal vs. External view
  - Stability vs. Responsiveness
  - Quality vs. Cost
  - Reactive vs. Proactive
- Service provision – A “culture of service”
- Lifecycle involvement – integral part of the lifecycle
- Assessing operational health – timely intervention
- Communications – up/down – in/out
- Documentation – key to a learning organization

Principles of Service Operation

In the book Alice in Wonderland, Alice and the Queen were discussing believing in impossible things. The Queen remarked that “Why, sometimes I’ve believed as many as six impossible things before breakfast.” This quote often seems to describe Service Operation as it tries to achieve an overall balance between a number of very strong opposing forces.

Service Operation demands a service provider wholeheartedly embrace a “culture of service.” It must actively participate in all aspects of the Service Lifecycle because Service Operation must live and operate with the decisions and actions made elsewhere.

Communication, both up and down as well as in and out of the organization, is key to achieving high levels of performance from the functions and processes of Service Operation.Further leading the way ,it promotes the documentation of its collective actions. This results in the IT service provider become a learning organization, not one dependant on “tribal knowledge.”



Organizing Service Operation

- Function
- Group
- Team
- Department
- Division
- Role

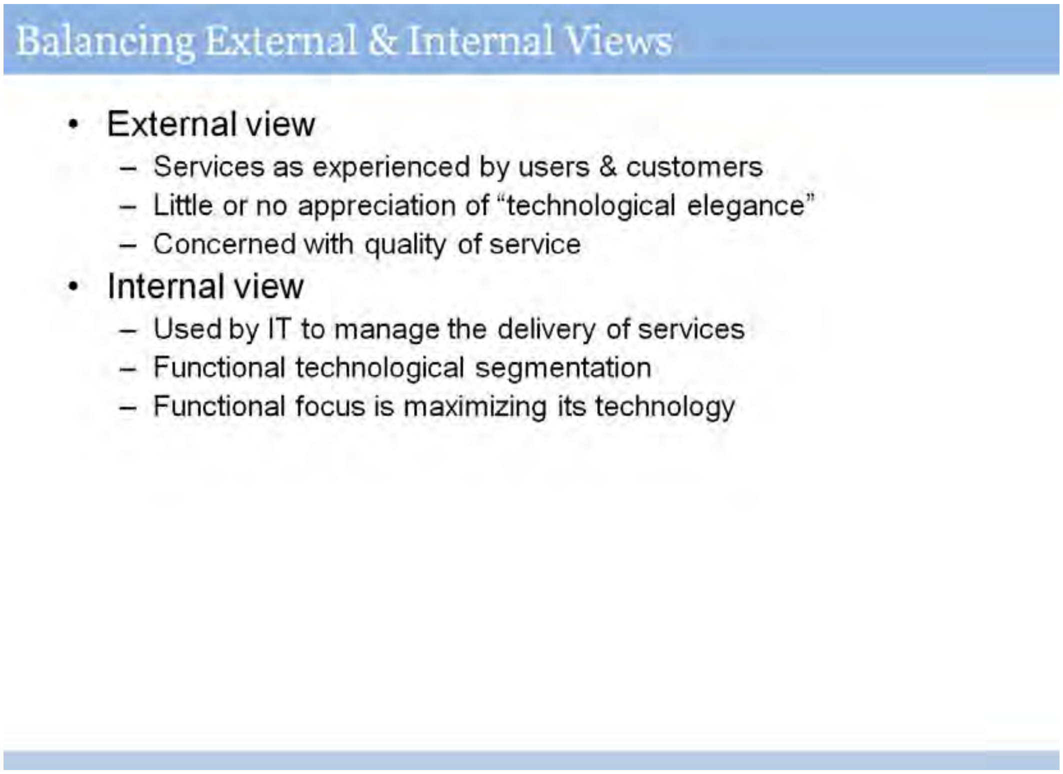
Organizing Service Operation

A key observation about organizing Service Operation is that there are many organizational compositions the service provider must address.

A function represents a team or group of people and the tools it uses to carry out one or more processes or activities. Groups and teams are groups of people assembled to perform a specific function or task. Although these terms lack standard definitions, a group is often an informal collection of staff knowledgeable about a particular issue or function, and a team is usually a formally designated group of people assigned to a particular function. The members of a team or group do not necessarily reside in the same department, but work together with staff from several departments.

Departments and divisions connote organizational structures, each of which has its own hierarchy of responsibilities and control. The exact nature of departments and divisions differs in every organization, depending on its size, business structure, location and corporate culture.

A role is a set of responsibilities, activities and authorities granted to a person or team. A role is defined within a process. A function may include many individual roles, and, in turn, a function may play a role within a larger process or activity.



Balancing External & Internal Views

- External view
  - Services as experienced by users & customers
  - Little or no appreciation of "technological elegance"
  - Concerned with quality of service
- Internal view
  - Used by IT to manage the delivery of services
  - Functional technological segmentation
  - Functional focus is maximizing its technology

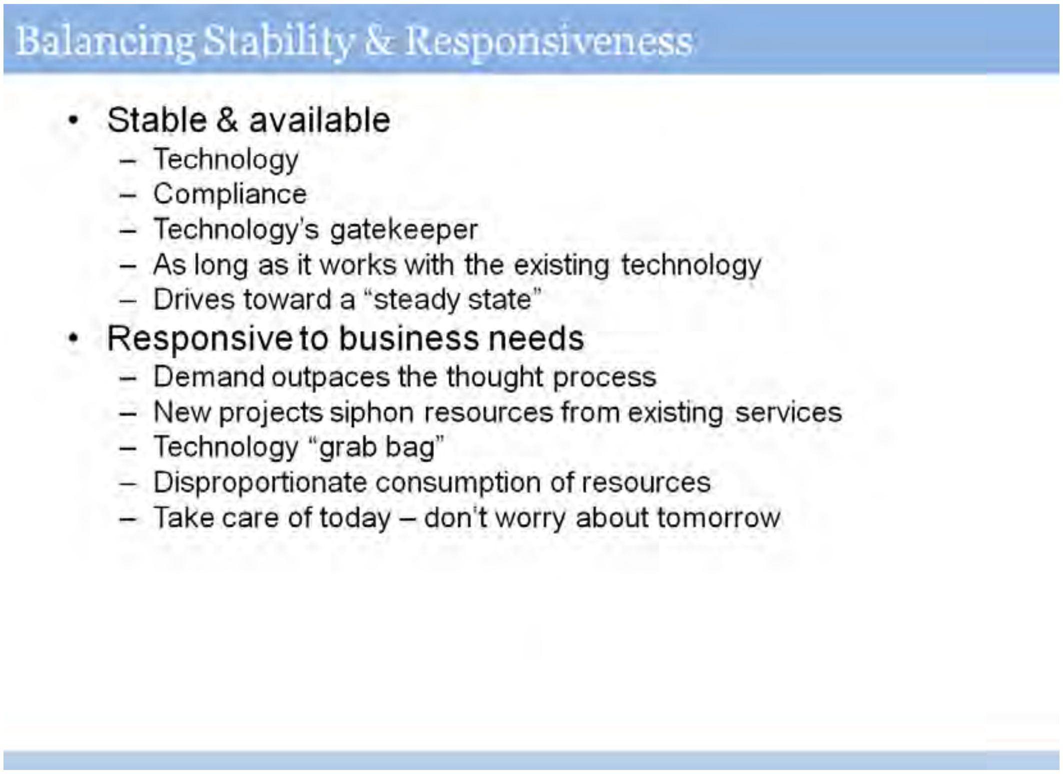
Balancing External & Internal Views

ITIL defines a service as "a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks." This affords us some insight into the difficulty Service Operation faces in balancing its "internal view" of a service with the customer's "external view" of the same service.

The external view of a service is from the perspective of the business customers and users who "consume" the service; it is their experience with the service.They neither know, nor care, what elegant combinations of hardware, software and engineering genius go into its delivery (nor should they). They experience only the utility and warranty of the service.

On the other hand, IT's internal view of the service is of all of those elegant pieces of hardware and wonderfully written software programs supported by really great tools that make it all work together. Moreover, because most of that elegant technology belongs to vertically integrated functional groups, it is often difficult for one group to see (or care) what other elegant pieces of hardware or software come from other groups.

Although the two views above represent the opposite ends of the spectrum, the challenge is to make sure the IT organization can meet the demands of the business and not under-deliver on its promises to the business.



Balancing Stability & Responsiveness

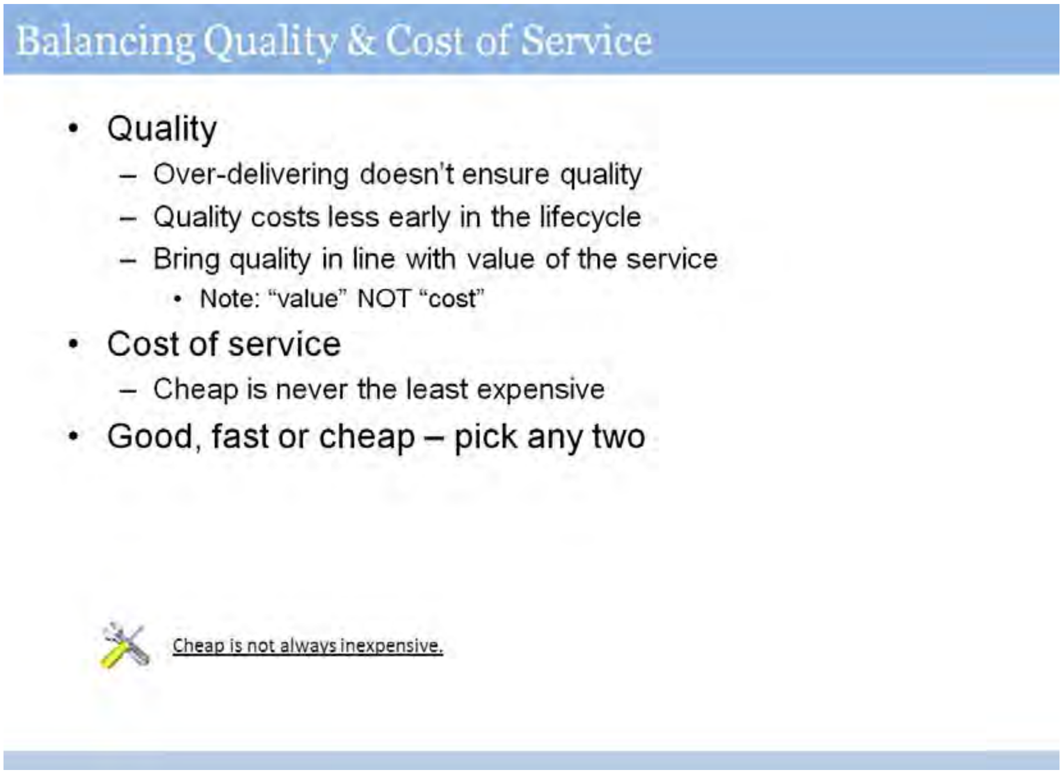
- Stable & available
  - Technology
  - Compliance
  - Technology's gatekeeper
  - As long as it works with the existing technology
  - Drives toward a "steady state"
- Responsive to business needs
  - Demand outpaces the thought process
  - New projects siphon resources from existing services
  - Technology "grab bag"
  - Disproportionate consumption of resources
  - Take care of today – don't worry about tomorrow

Balancing Stability & Responsiveness

Striking the balance between being responsive to the business while maintaining a stable IT infrastructure and high service availability is a challenging goal to achieve. The business wants to implement changes right away, while IT appreciates the contribution a "steady state" makes to its quality of service (QoS) objectives.

This ongoing demand for changes to technology-enabled business processes can result in a patchwork of infrastructure that places a disproportionate demand on IT resources.

If left unchecked, this environment creates a situation in which many IT organizations act more as "gatekeepers" than service providers. IT finds itself relegated to maintaining the status quo (stable infrastructure) at the cost of responding to the business' need for change. The short-term objectives often seem to outweigh the long-term strategies.



Balancing Quality & Cost of Service

- Quality
  - Over-delivering doesn't ensure quality
  - Quality costs less early in the lifecycle
  - Bring quality in line with value of the service
    - Note: "value" NOT "cost"
- Cost of service
  - Cheap is never the least expensive
- Good, fast or cheap – pick any two

Cheap is not always inexpensive.

Balancing Quality & Cost of Service

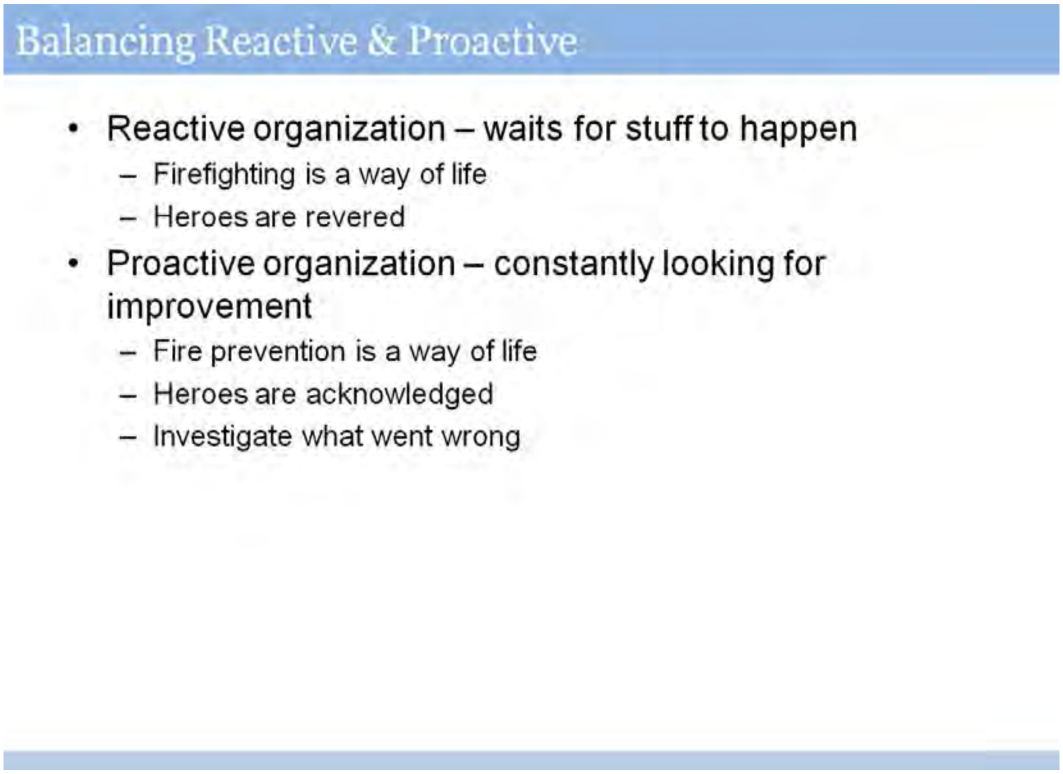
Life is full of compromises, and balancing the quality of something with its cost creates difficulty for many IT service providers and businesses.

We have all heard the saying, "You can have it good, fast or cheap. Pick any two." The difficulty comes in balancing Quality of Service (QoS) with the Cost of Service (CoS) while viewing "good," "fast" and "cheap" as absolutes.

Goodness and quality are, in effect, the same; the ability of a product, service or process to provide the intended value. How quickly IT can deliver a product, service or process is a direct function of resources, which impact time-to-deliver and cost. Increase one and something, somewhere, must change to accommodate it.

Balancing QoS and CoS focuses on bringing quality in line with the value of the service, NOT its cost! Many businesses tend to confuse cost and value and end up seeing service quality fall off after across-the-board cost-cutting. One basic truth in IT Service Management is "cheap" NEVER ends up being least expensive.

> Often Service Provider organizations base their decisions primarily on cost. When this happens at the expense of other considerations such as time or quality, hidden costs end up exceeding any apparent savings in cost. Therefore, the cheapest approach to doing something is not always the least expensive.



Balancing Reactive & Proactive

- Reactive organization – waits for stuff to happen
  - Firefighting is a way of life
  - Heroes are revered
- Proactive organization – constantly looking for improvement
  - Fire prevention is a way of life
  - Heroes are acknowledged
  - Investigate what went wrong

Balancing Reactive & Proactive

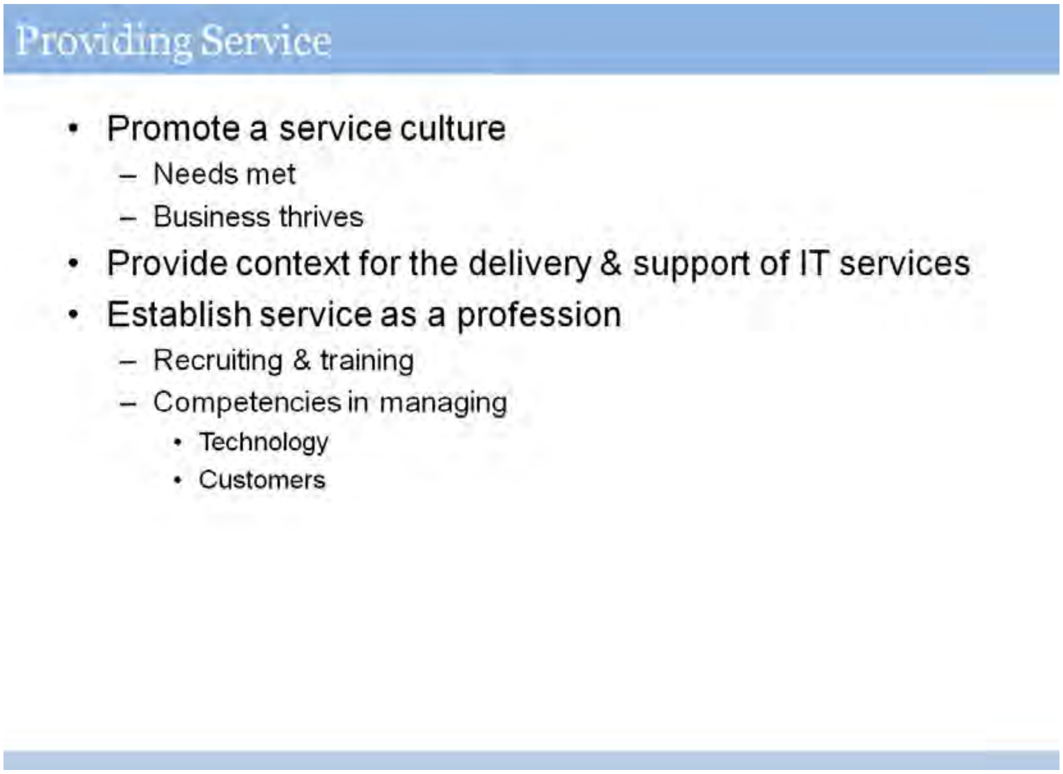
Any IT professional who has been around for any length of time has probably accumulated a whole drawer full of “hero badges.” These are the accolades or kudos bestowed upon our IT service provider's heroes for rushing in and saving the day through their extraordinary efforts.

In a “reactive organization,” where fire fighting is the normal way of life, the heroes are revered, get big raises and coveted promotions. But organizations that are constantly fire fighting tend to consume their valuable technical functional resources "fixing stuff” instead of "doing stuff” that would help the business be more successful.

A “proactive organization,” on the other hand, is always looking for ways to improve things. Here fire prevention is a way of life. Although heroes are recognized for their contribution to the organization, a proactive organization always investigates the situation that led to the need for a hero and sees if there are ways to avoid the use of heroism again.

Making the move to a proactive organization depends on a number of different things:

- The overall maturity of the IT organization
- The organizational culture
- IT’s role within the business
- Level of process and tool integration
- Maturity and scope of Knowledge Management



Providing Service

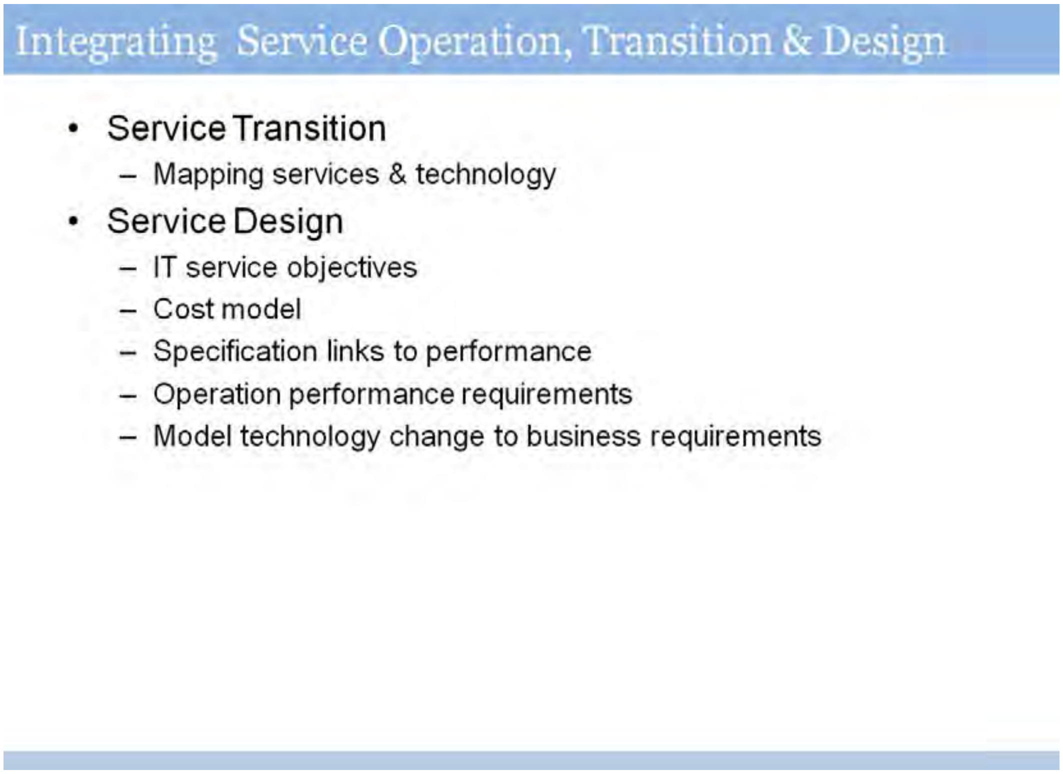
- Promote a service culture
  - Needs met
  - Business thrives
- Provide context for the delivery & support of IT services
- Establish service as a profession
  - Recruiting & training
  - Competencies in managing
    - Technology
    - Customers

Providing Service

The concept of a service culture undoubtedly manifests itself most clearly within the Service Operation portion of the Service Lifecycle. All of the other domains lay the foundation, but it is here that the service culture actually goes to work.

In short, a service culture recognizes that its major objective is customer satisfaction as it helps customers achieve their business objectives. Looking inward, this means that IT values its technical and performance achievements as mileposts in the journey to customer satisfaction.

IT achieves a service culture by making each staff member aware of the larger picture of business goals and objectives, and the value of his or her participation in it. IT must look upon service as a profession and adjust its performance metrics and recruitment requirements accordingly.

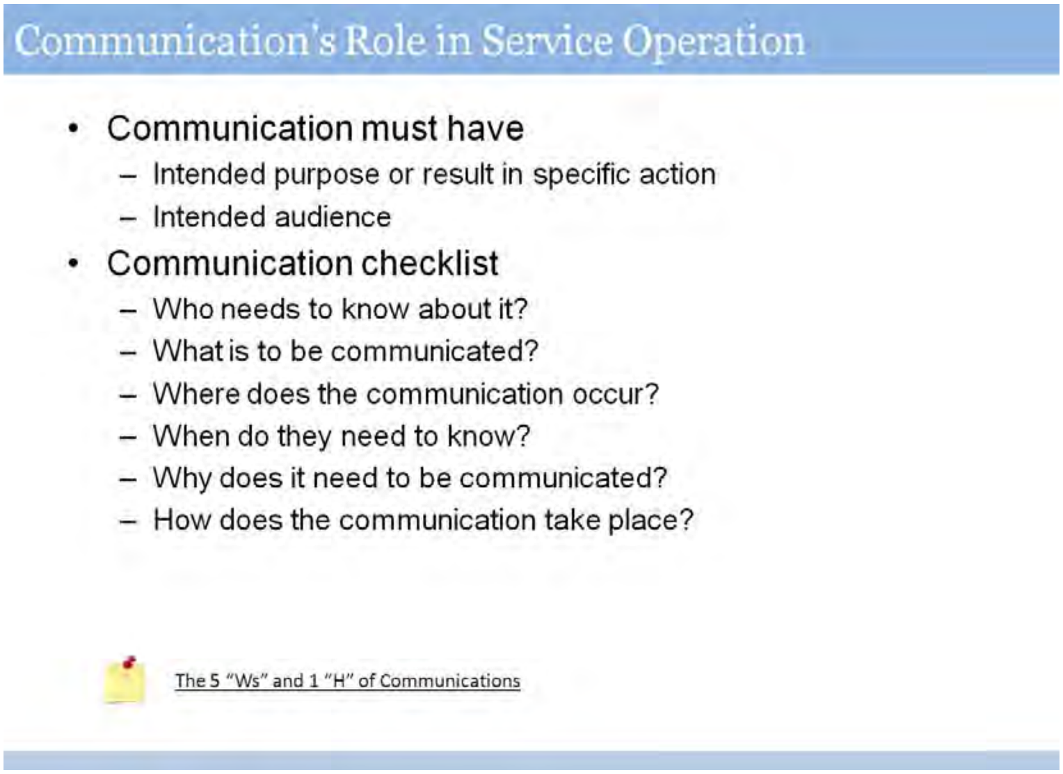


Integrating Service Operation, Transition & Design

- Service Transition
  - Mapping services & technology
- Service Design
  - IT service objectives
  - Cost model
  - Specification links to performance
  - Operation performance requirements
  - Model technology change to business requirements

Integrating Service Operation, Transition & Design

In addition to performing daily Service Operation activities, Service Operation staff participate in Service Design and Service Transition activities. Occurring early in the Service Design and Service Transition stages, this participation ensures that new services are fit for purpose from a Service Operation perspective,are supportable, and integrate with Service Transition capabilities.



Communication's Role in Service Operation

- Communication must have
  - Intended purpose or result in specific action
  - Intended audience
- Communication checklist
  - Who needs to know about it?
  - What is to be communicated?
  - Where does the communication occur?
  - When do they need to know?
  - Why does it need to be communicated?
  - How does the communication take place?

The 5 “Ws” and 1 “H” of Communications

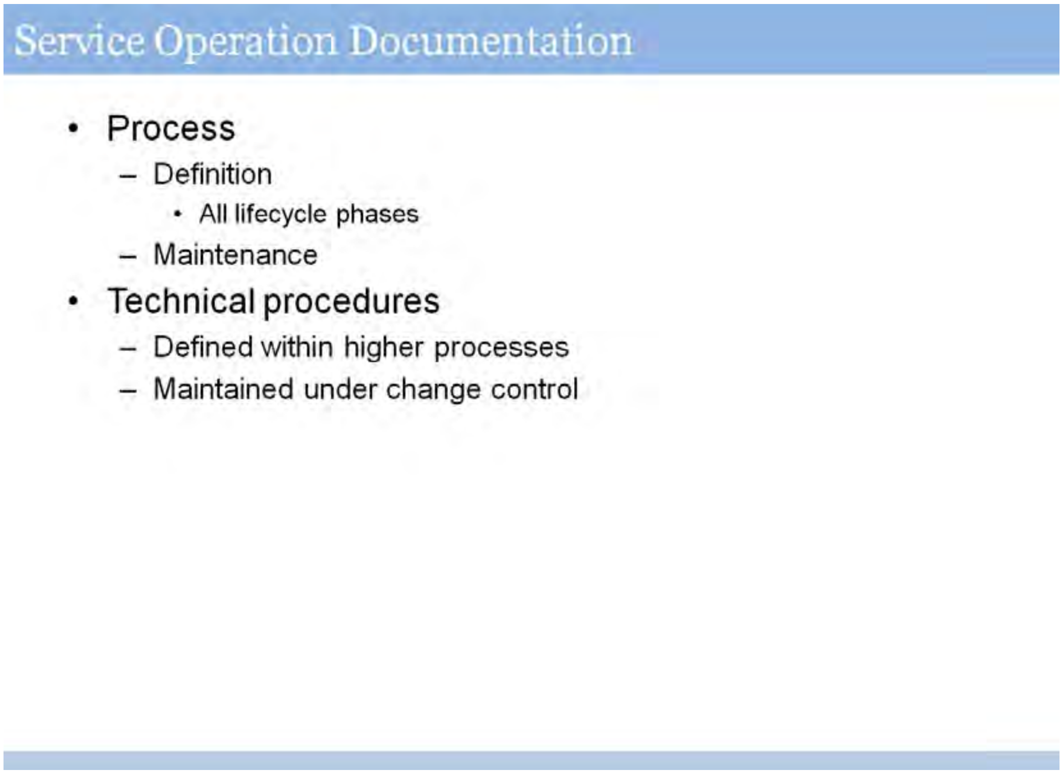
Communication's Role in Service Operation

In its daily activities, Service Operation communicates frequently with both internal and external recipients about topics such as inter-shift operations handover, performance and project reporting, changes, exceptions, emergencies, training on new processes and service designs, and strategy and design information for internal Service Operation teams.

The most important thing to remember about communication is that it derives from the word "to commune" or "to share." In other words, communication must always be a two-way process. It must always have an intended audience, and it must always communicate the message to the audience in the language and method the audience expects.

The most effective communication relies on a checklist similar to the journalist's credo of Who? What? Where? When? Why? and How? A successful communications document or campaign answers each of these questions and specifically targets its intended audience.

The 5 "Ws" and 1 "H" of Communications– **Who**? Who is the communication intended for? Who initiated the communication? **What**? What is the topic of the communication? **Where**? Where does the communication apply? What is its scope? **When**? When does the subject topic of the communication take place? In the future? Has it already happened? **Why**? Why is it necessary to release the communication? Does the recipient need to do or know something? **How**? How will the subject topic of the communication happen? Does the communication need to include instructions for doing something?



Service Operation Documentation

- Process
  - Definition
    - All lifecycle phases
  - Maintenance
- Technical procedures
  - Defined within higher processes
  - Maintained under change control

Service Operation Documentation

Documentation is one of the keys to ensuring the consistent execution of operations procedures and activities. Service Operation documentation breaks down into four areas.

Standard Operation Procedures, known as SOPs, represent the detailed instructions the operations staff follows in the day-to-day execution of the procedures and activities of managing the IT infrastructure. The scope of SOPs extends over all of the devices and systems under management, and includes defined standards of performance. Operational Level Agreements (OLAs) often reference these performance standards.

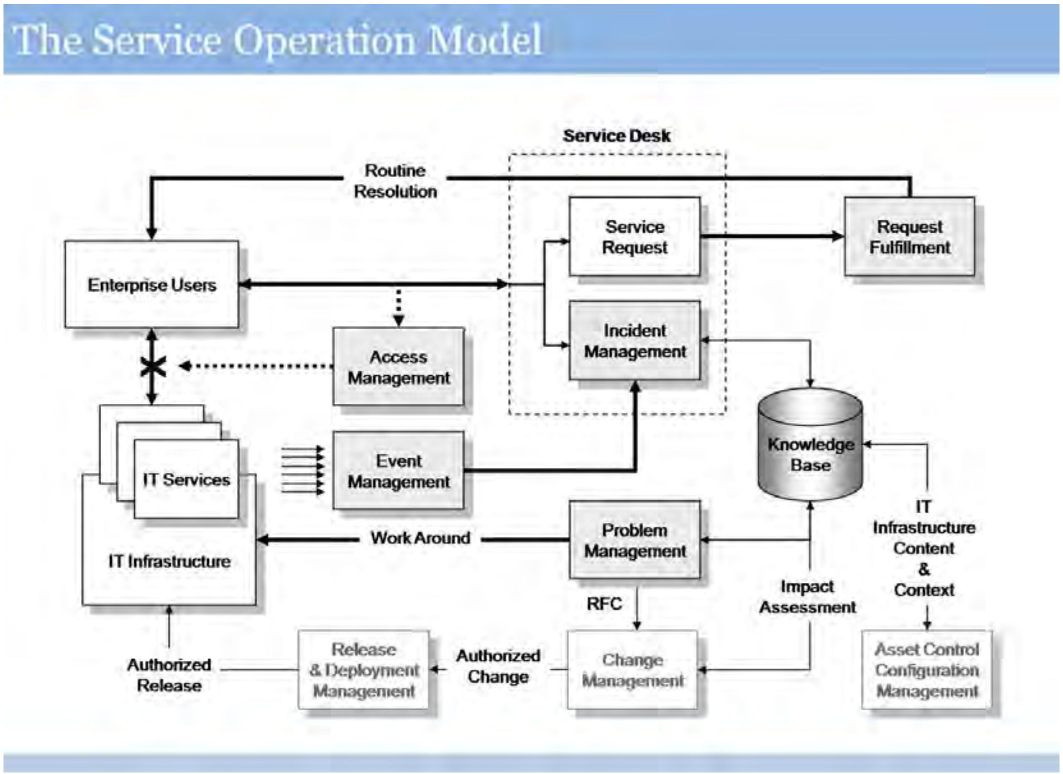
Operations logs record what was done, by whom, when and what the outcomes were. The logs provide the “paper trail” for the execution of operations procedures. They can be in hardcopy written form or electronic, and must be covered by a policy that includes guidance on the retention of the logs.

Shift schedules and reports document the schedule of activities that the Operations staff carry out in each shift. It coordinates activities across multiple shifts and ensures consistency in their execution. Tools used to support operations scheduling can be as simple as a handwritten sheet of paper or as sophisticated as an enterprise scheduling product.

Operations schedules provide a high-level overview of planned operations. They not only include normal operations activities, but also outline changes to routine jobs, anything added on a one-off basis, and scheduled maintenance by Technical Management staff or external service providers.

Lesson 10

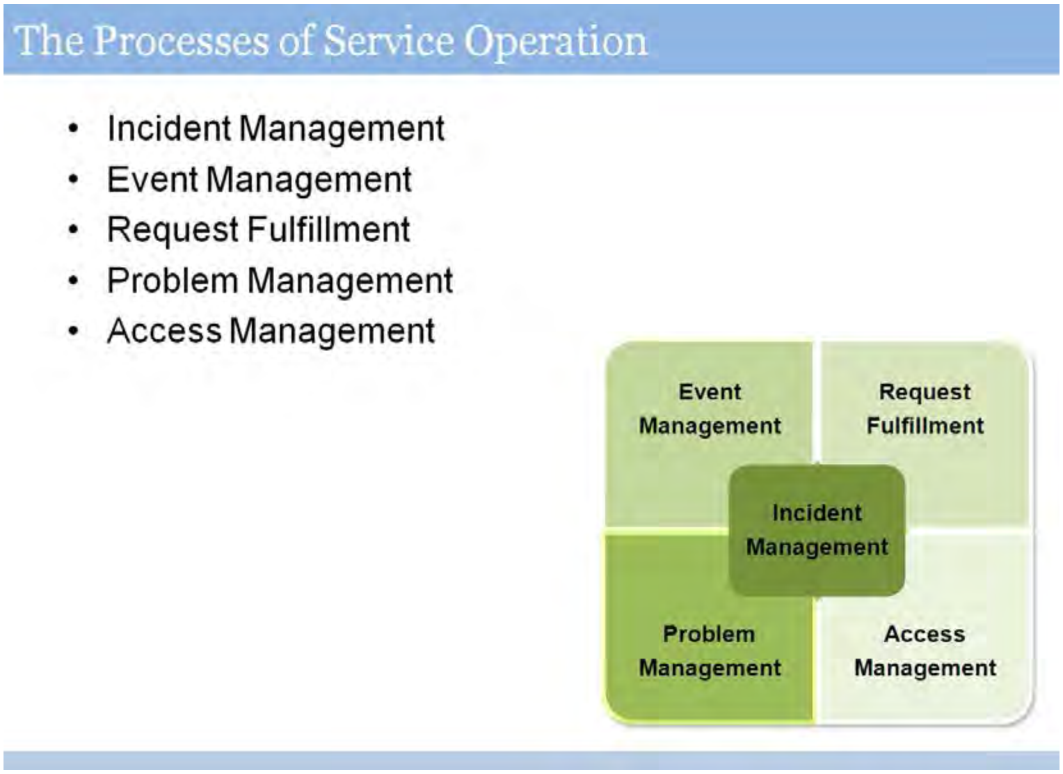
Service Operation Processes



The Service Operation Model

The Service Operation Model

This is a high-level diagram of how the functions and processes of Service Operation relate to each other, other Service Lifecycle processes and the business users.



The Processes of Service Operation

- Incident Management
- Event Management
- Request Fulfillment
- Problem Management
- Access Management

Event Management

Request Fulfillment

Incident Management

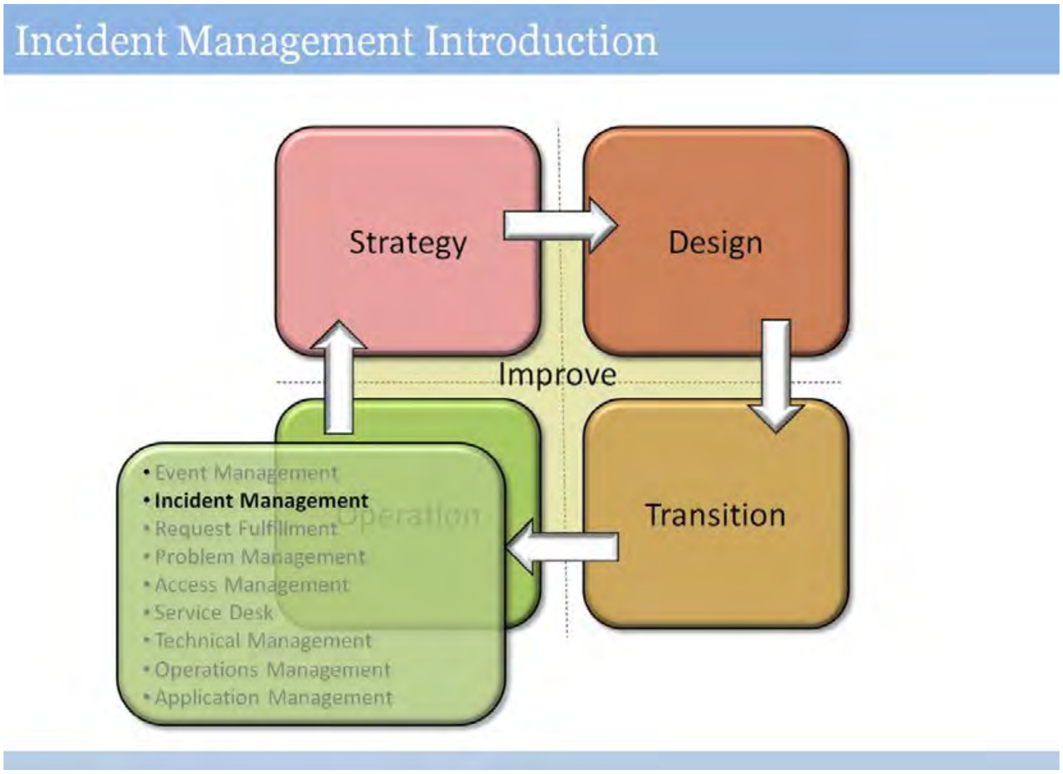
Problem Management

Access Management

The Process of Service Operation

The five Service Operation processes will be examined in the following sections.

- Incident Management - Coordination of IT resources needed to restore an IT service.
- Event Management - Monitoring events throughout the IT Infrastructure.
- Request Fulfillment - Managing customer & user requests that are not the result of an incident.
- Problem Management - Finding the root cause of events & incidents.
- Access Management - Granting authorized users the right to use a service.



Incident Management Introduction

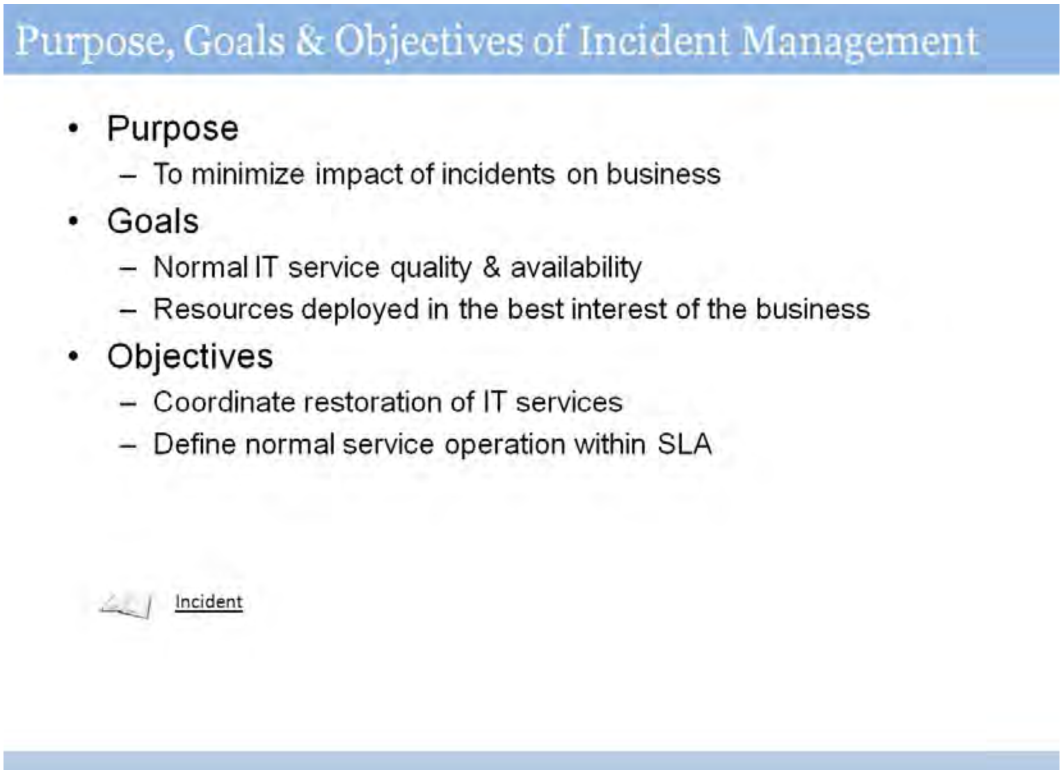
- Event Management
- **Incident Management**
- Request Fulfillment
- Problem Management
- Access Management
- Service Desk
- Technical Management
- Operations Management
- Application Management

Incident Management Introduction

The Incident Management process is normally the responsibility of the Service Desk function. Its objective is to coordinate the rapid restoration of IT services. By itself, Incident Management does not repair any failed component within the IT infrastructure. Its sole purpose is to coordinate that effort through other functional areas within the IT Service Provider's organization.

Many IT organizations mistakenly identify the Incident Management process activities as Problem Management. While seemingly insignificant on the surface, the objectives of the two processes are quite dissimilar. The IT Infrastructure Library forces rigorous definitions of both terms and processes to help IT organizations better understand, and communicate.

Many organizations create Incident Models that pre-define the steps for handling particular types of incidents that may reoccur. Incident Models document the steps the Incident Management process should follow, who holds responsibility for various actions in the Incident process, time scales and thresholds for completion of actions, and escalation procedures.



Purpose, Goals & Objectives of Incident Management

- Purpose
  - To minimize impact of incidents on business
- Goals
  - Normal IT service quality & availability
  - Resources deployed in the best interest of the business
- Objectives
  - Coordinate restoration of IT services
  - Define normal service operation within SLA

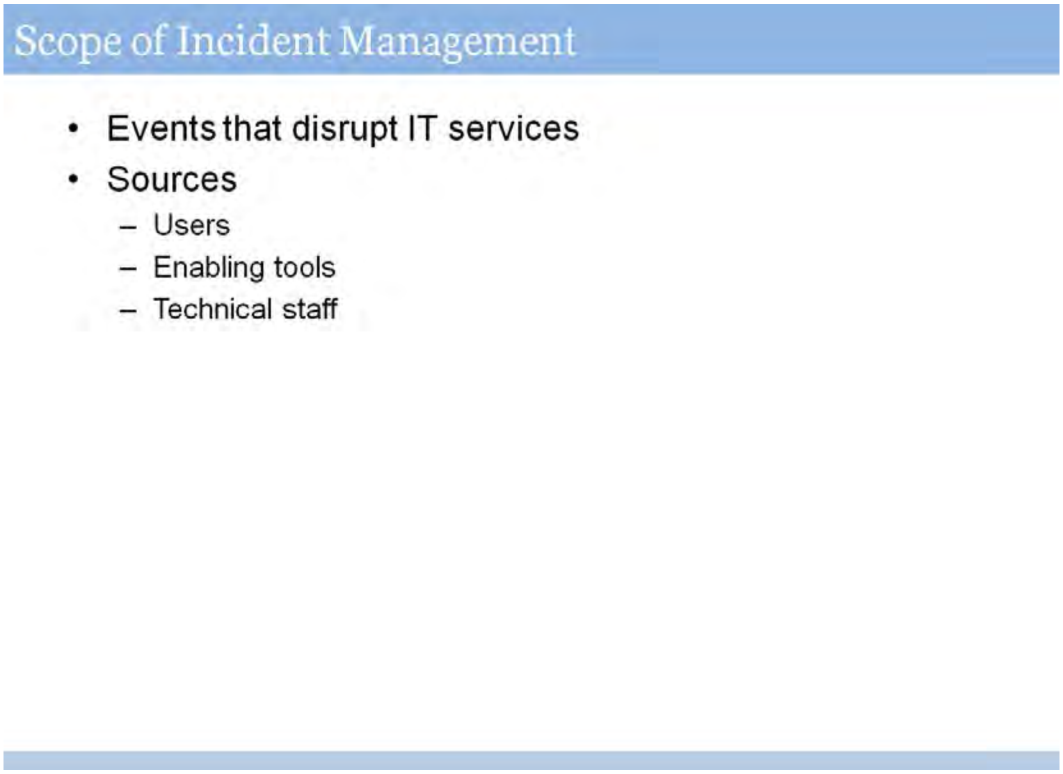
Incident

Purpose, Goals & Objectives of Incident Management

The Incident Management process minimizes the impact an IT Service failure has on the business. It seeks to maintain IT Service quality and availability. It also optimizes the Service Provider's ability to deploy its staff in the best interests of the business.

It accomplishes its goals by coordinating resources and assets to efficiently and effectively restore IT Services within the service boundaries established within the Service Level Agreement.

An incident is an unplanned interruption to an IT Service or reduction in the quality of an IT Service. Failure of a configuration Item that has not yet affected service is also an incident.



Scope of Incident Management

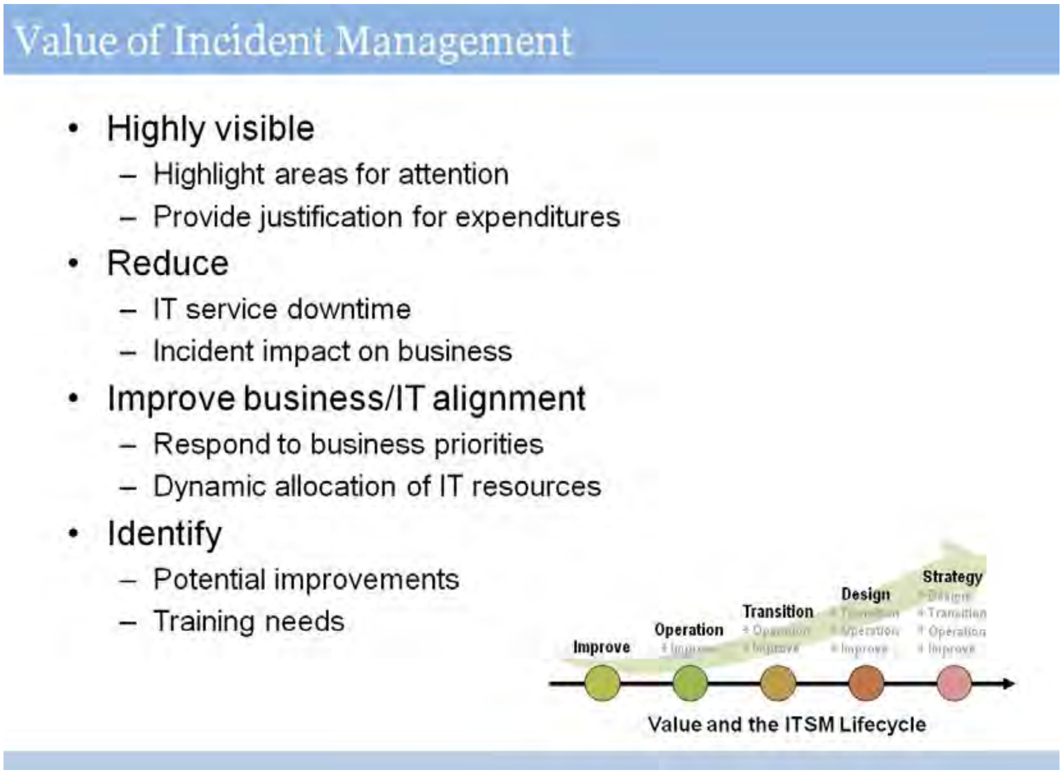
- Events that disrupt IT services
- Sources
  - Users
  - Enabling tools
  - Technical staff

Scope of Incident Management

The scope of Incident Management extends over any event within the IT infrastructure that disrupts an IT Service. This concept extends even to events that by themselves do not represent an outage, but may cause a degraded service or put a service at risk

An example might be the loss of a disk drive's mirrored drive. Although the event may not disrupt the service, the service is at risk of disruption should the primary disk drive fail. An example of a degraded service might be the loss of one of the dual input/output (I/O) channels to a disk array. While, as in the previous example, the service may be at risk should the other channel fail, the failed channel may reduce overall throughput, adversely affecting the service's performance.

Detecting and reporting Incidents may derive from many different sources, including both users and availability- and performance-monitoring tools. In addition, as part of its normal daily activities, the technical staff of the IT organization may become aware that something is amiss and is impacting or putting an IT Service at risk of disruption.



Value of Incident Management

- Highly visible
  - Highlight areas for attention
  - Provide justification for expenditures
- Reduce
  - IT service downtime
  - Incident impact on business
- Improve business/IT alignment
  - Respond to business priorities
  - Dynamic allocation of IT resources
- Identify
  - Potential improvements
  - Training needs

Improve
Operation
+ Improve
Transition
+ Operation
+ Improve
Design
+ Transition
+ Operation
+ Improve
Strategy
+ Design
+ Transition
+ Operation
+ Improve

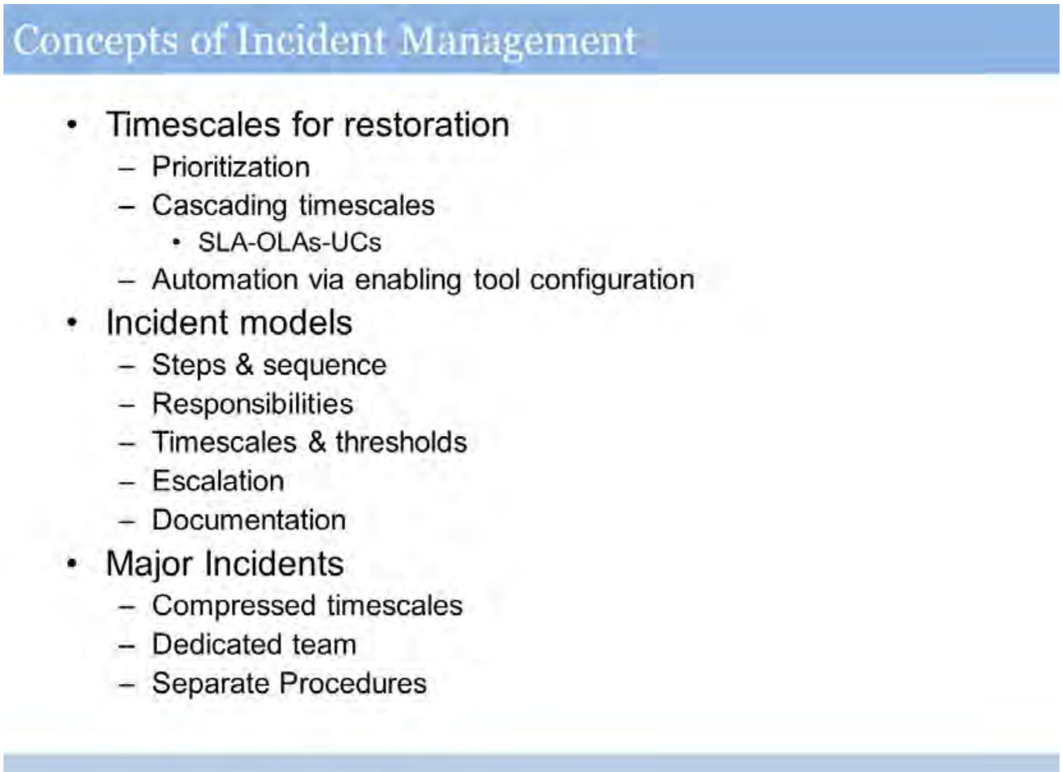
Value and the ITSM Lifecycle

Value of Incident Management

From the business perspective, Service Operation lies at the heart of realizing IT Service value. The Incident Management process becomes a highly visible area of attention for the business when "things break." A well-managed Incident Management process sets the stage for, or can provide the justification for, adequate funding of the entire set of Service Operation processes and functions.

The business realizes (captures) the value of IT Service through Incident Management whenever it steps up to address IT Service downtime, thereby reducing a disruption's negative impact to the business. It also provides a flexible mechanism to dynamically allocate IT resources in response to business priorities.

Finally, Incident Management provides the context for identifying potential improvements to IT Services and to IT and business user training needs.



Concepts of Incident Management

- Timescales for restoration
  - Prioritization
  - Cascading timescales
    - SLA-OLAs-UCs
  - Automation via enabling tool configuration
- Incident models
  - Steps & sequence
  - Responsibilities
  - Timescales & thresholds
  - Escalation
  - Documentation
- Major Incidents
  - Compressed timescales
  - Dedicated team
  - Separate Procedures

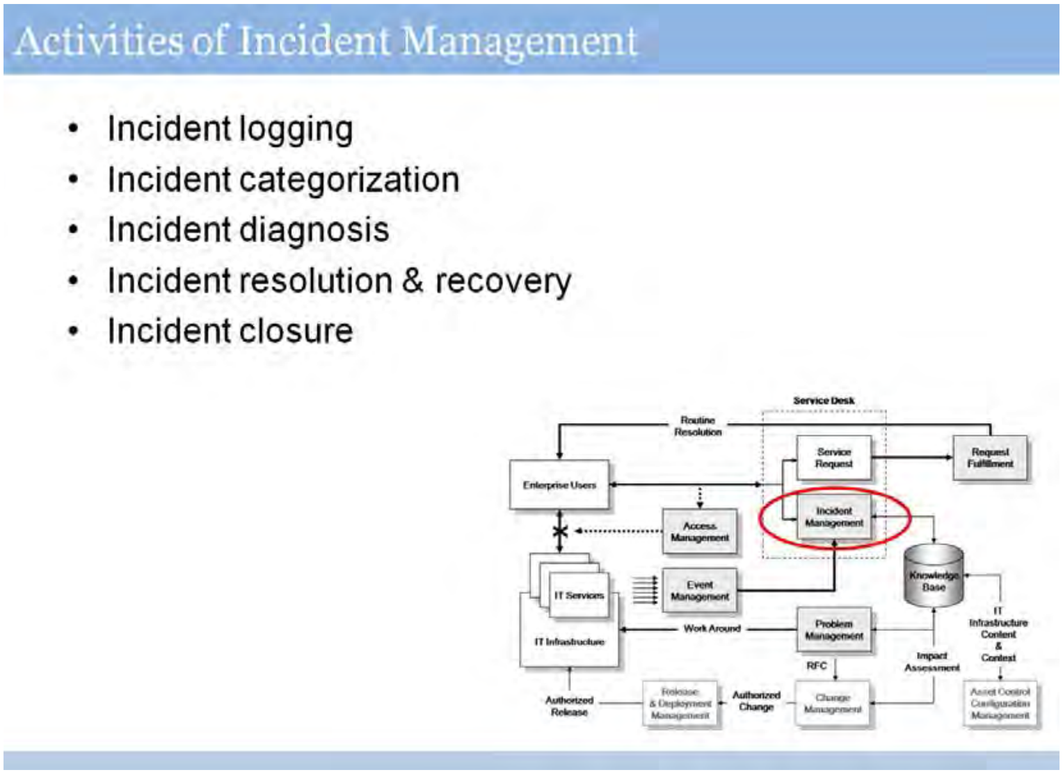
Concepts of Incident Management

Fundamental to the Incident Management process is the idea that not all incidents are equal, and, therefore, they do not require the same level of response in the same time frame. An incident's priority (business impact & urgency) dictates the IT organization's response and the subsequent deployment of its resources.

Incident Management response time frames support the targets specified within the relevant Service Level Agreements (SLA). Within the IT organization, as well as any external product or service provider, Operational Level Agreements (OLA) and Underpinning Contracts (UC) must also support the SLA's restoration targets. Enabling tools can automate this to a certain extent.

Very seldom do IT organizations run into something brand new. They have seen most of the incidents that occur, and they will see them again. To aid in the rapid restoration of IT Services, an IT organization can create Incident Models that lay out the progression of steps for restoring a service, staff involvement and responsibilities, timescale, criteria for escalation, and required documentation.

Major Incidents are Incidents that either have, or will have, a major impact on the business. They operate with compressed timeframe for restoring the service, and often a dedicated team oversees the restoration effort. There is normally a separate set of procedures for handling Major Incidents.



Activities of Incident Management

- Incident logging
- Incident categorization
- Incident diagnosis
- Incident resolution & recovery
- Incident closure

Service Desk
Routine Resolution
Service Request
Request Fulfillment
Enterprise Users
Incident Management
Access Management
Knowledge Base
IT Services
Event Management
IT Infrastructure
Work Around
Problem Management
IT Infrastructure Content & Context
RFC
Impact Assessment
Authorized Release
Release & Deployment Management
Authorized Change
Change Management
Asset Control Configuration Management

Activities of Incident Management

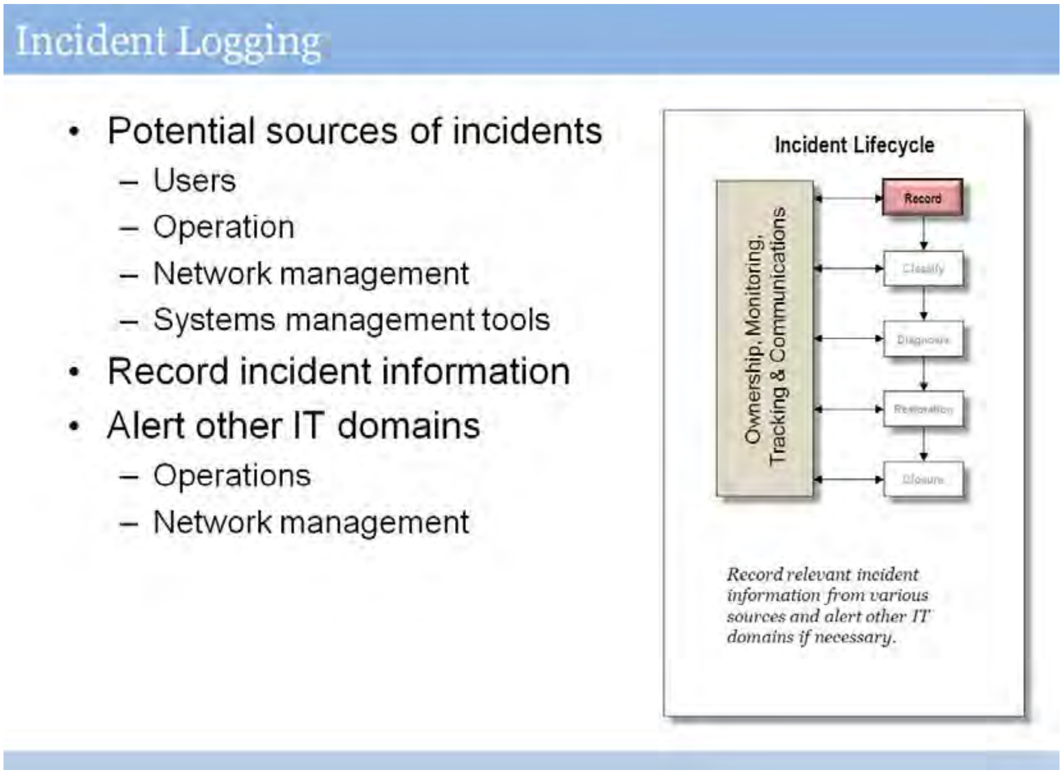
The activities of the Incident Management process perform the full lifecycle of the Incident.

Incident Logging captures basic information about the Incident and records it in the Incident database. Incident Categorization gathers more information about it, determines what portion of the infrastructure it is impacting, assigns priority, and attempts to match its symptoms to a knowledge database.

During Incident Diagnosis, Incident Management coordinates the investigation of the incident, escalates it if needed, coordinates the development of a workaround if available, and maintains constant communication with the user.

Incident Resolution & Recovery applies workarounds, updates any knowledge database matches, oversees any service restoration activity and updates the Incident record.

Finally, the Incident Closure activity performs a final review to determine that service has been restored to the user, does a final classification of the Incident and closes the Incident record.



Incident Logging

- Potential sources of incidents
  - Users
  - Operation
  - Network management
  - Systems management tools
- Record incident information
- Alert other IT domains
  - Operations
  - Network management

Record relevant incident information from various sources and alert other IT domains if necessary.

Incident Logging

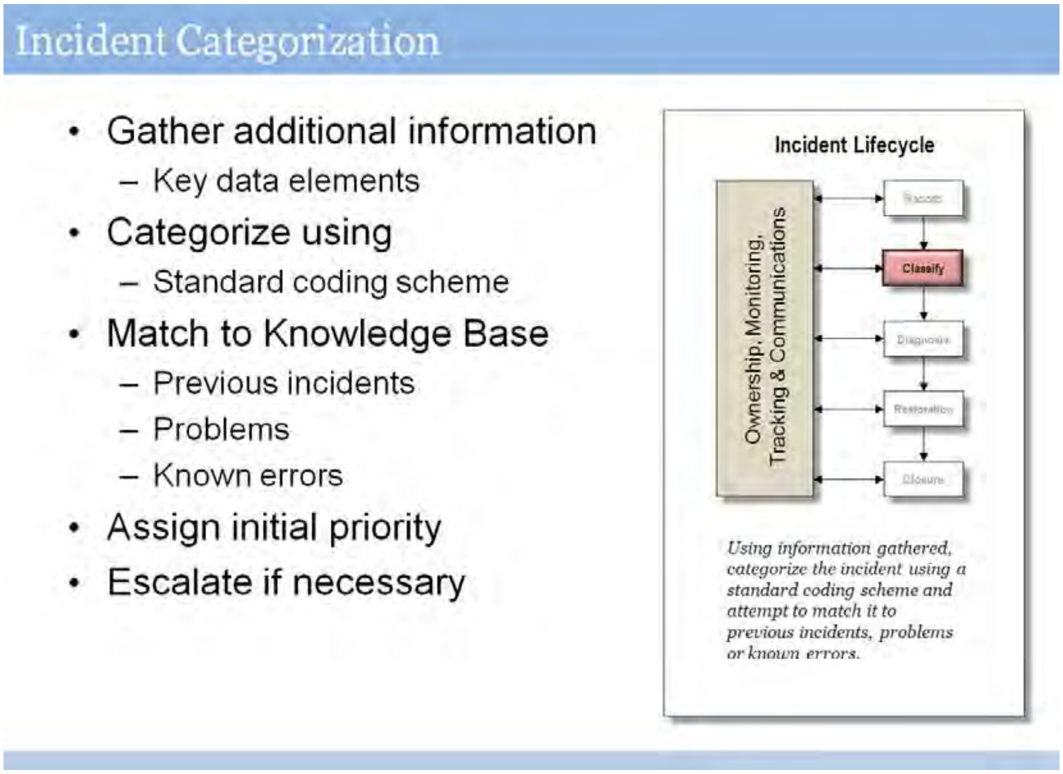
The definition of an Incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a Configuration Item (CI) that has not yet affected service is also an Incident.

The definition of an Incident includes anything that is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity. Thus, a degraded IT service could be an Incident, just as if that service were totally down.

The most common source of Incidents is users calling the Service Desk, and the operations group also commonly reports Incidents. Network and Systems Management and monitoring tools can provide automatic event notification directly to an automated Incident management system.

Once detected, the Incident Lifecycle begins by recording the details of the Incident. It creates an Incident Record that links to the Incident and the affected CIs in the Configuration Management System (CMS).

Incident Management often receives the first notification of an Incident from the users; i.e., physical damage such as lightning strikes. In these cases, it is common for Incident Management to alert other IT domains. Throughout the entire Incident Management Lifecycle, Incident Management staff updates the Incident Record as additional information becomes available, and the Service Desk maintains continual contact with the user.



Incident Categorization

- Gather additional information
  - Key data elements
- Categorize using
  - Standard coding scheme
- Match to Knowledge Base
  - Previous incidents
  - Problems
  - Known errors
- Assign initial priority
- Escalate if necessary

Incident Lifecycle

Ownership, Monitoring,
Tracking & Communications
Record
Classify
Diagnosis
Restoration
Closure

Using information gathered, categorize the incident using a standard coding scheme and attempt to match it to previous incidents, problems or known errors.

Incident Categorization

This activity gathers information, identifies the characteristics of an Incident, and matches it to previous Incidents, Problems and Known Errors. Gathering information facilitates diagnosis, but does not determine the root cause of the Incident.

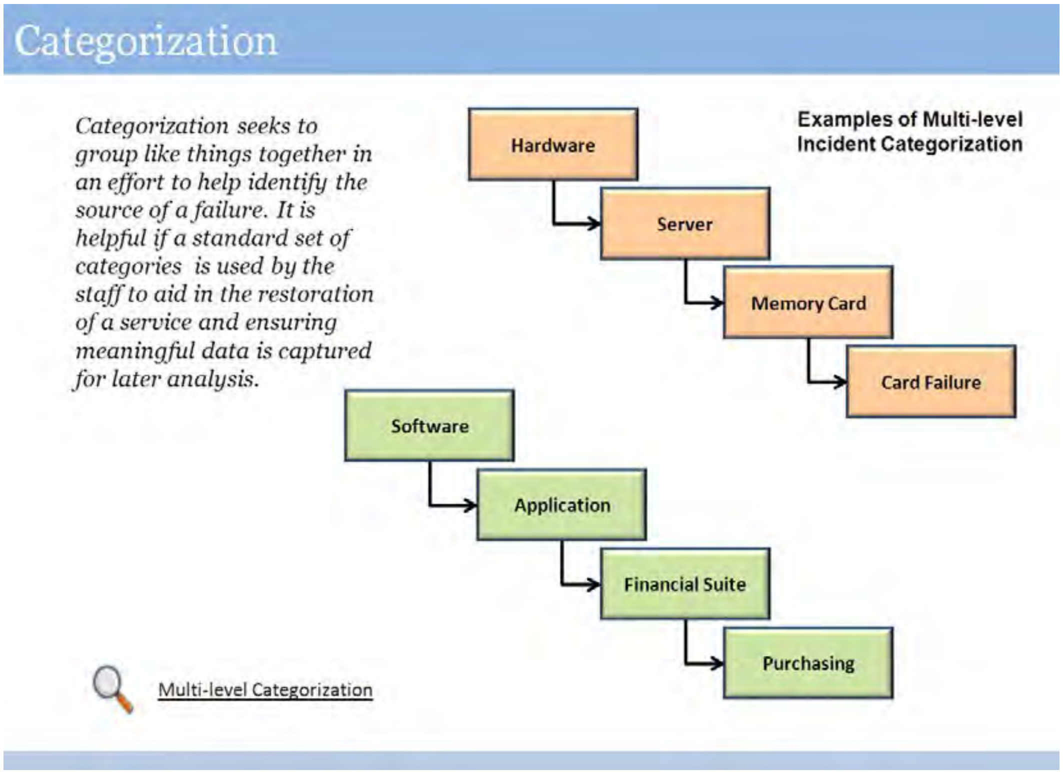
Categorization identifies an Incident by origin and symptoms and assigns a standard priority based on business impact and urgency. It references the Service Level Agreements (SLA) for this information.

The Service Knowledge Management System (SKMS) stores Incidents, Problems, and Known Errors as part of a “knowledge base.” Matching an incident to the knowledge base provides a resolution or a Workaround. The SKMS maintains known errors in the Known Error Database (KEDB).

The Incident Matching activity uses these common terms:

- ***Workaround***– the interim reduction of impact or elimination of an Incident or Problem for which a full resolution is not yet available
- ***Problem*** – a cause of one or more Incidents
- ***Known Error*** - a Problem that has a documented root cause and a workaround

When Incident Management needs higher-level support or more resources, it can escalate the Incident, making other areas within the business or IT aware of the situation.



Categorization

Categorization seeks to group like things together in an effort to help identify the source of a failure. It is helpful if a standard set of categories is used by the staff to aid in the restoration of a service and ensuring meaningful data is captured for later analysis.

Examples of Multi-level Incident Categorization

Hardware
Server
Memory Card
Card Failure

Software
Application
Financial Suite
Purchasing

Multi-level Categorization

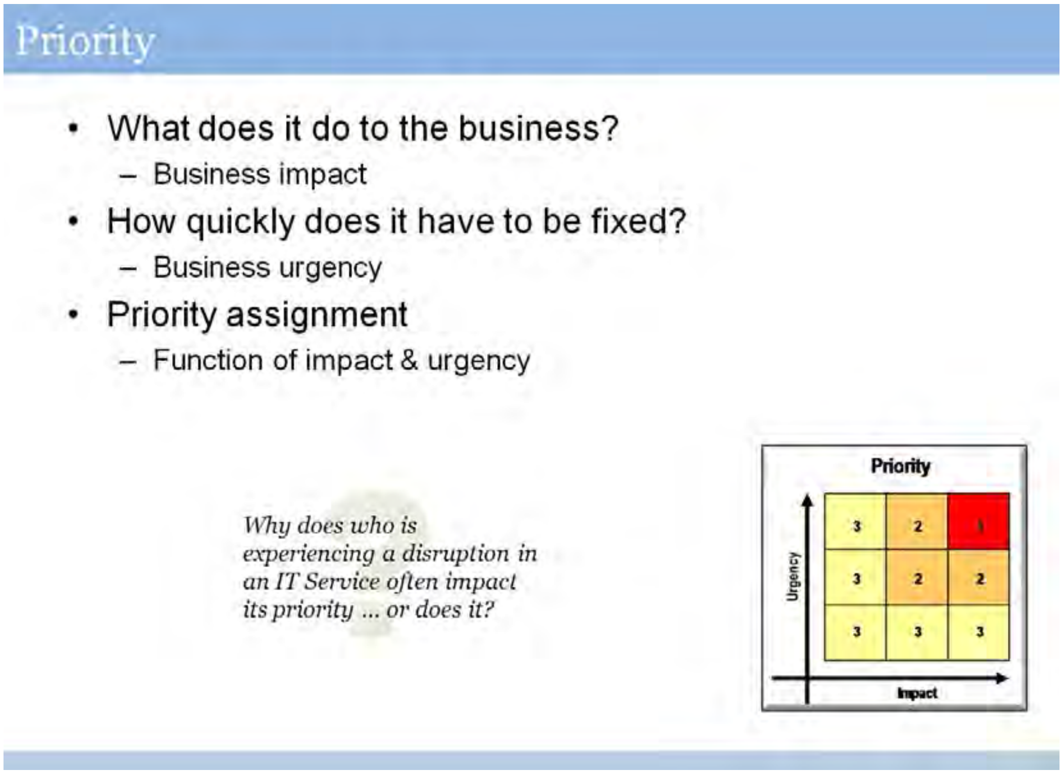
Categorization

Categorization (also known as classification) bounds which component of the infrastructure might be causing the disruption of an IT Service. A typical categorization scheme establishes a hierarchy of categories, and each subsequent level narrows the scope of possible infrastructure components

A categorization scheme is normally unique to each IT organization because the details of such schemes depend greatly on the size and complexity of the IT infrastructure. This requires each IT organization to figure it out “on its own.”

Although no specific guidance exists, generally the steps to arrive at a workable scheme involve gathering knowledgeable members of the IT staff, putting together a strawman” scheme, trying it out, analyzing the results and tweaking as required. Most enabling tools that support the Service Operation processes have the capability to support three or four levels of granularity. This is normally enough to provide the necessary scoping and data necessary to support the Incident and Problem Management processes.

Categorization is a technique used to group like things together. Multi-level categorization takes this technique one step further by "grouping like groups" together. By doing this a Service Provider can create meaningful groupings of things (components of the infrastructure) to aid in quickly identifying which portion of the infrastructure might be involved in an incident or problem.



Priority

- What does it do to the business?
  - Business impact
- How quickly does it have to be fixed?
  - Business urgency
- Priority assignment
  - Function of impact & urgency

Why does who is experiencing a disruption in an IT Service often impact its priority ... or does it?

Priority
Urgency
Impact

3	2	1
3	2	2
3	3	3

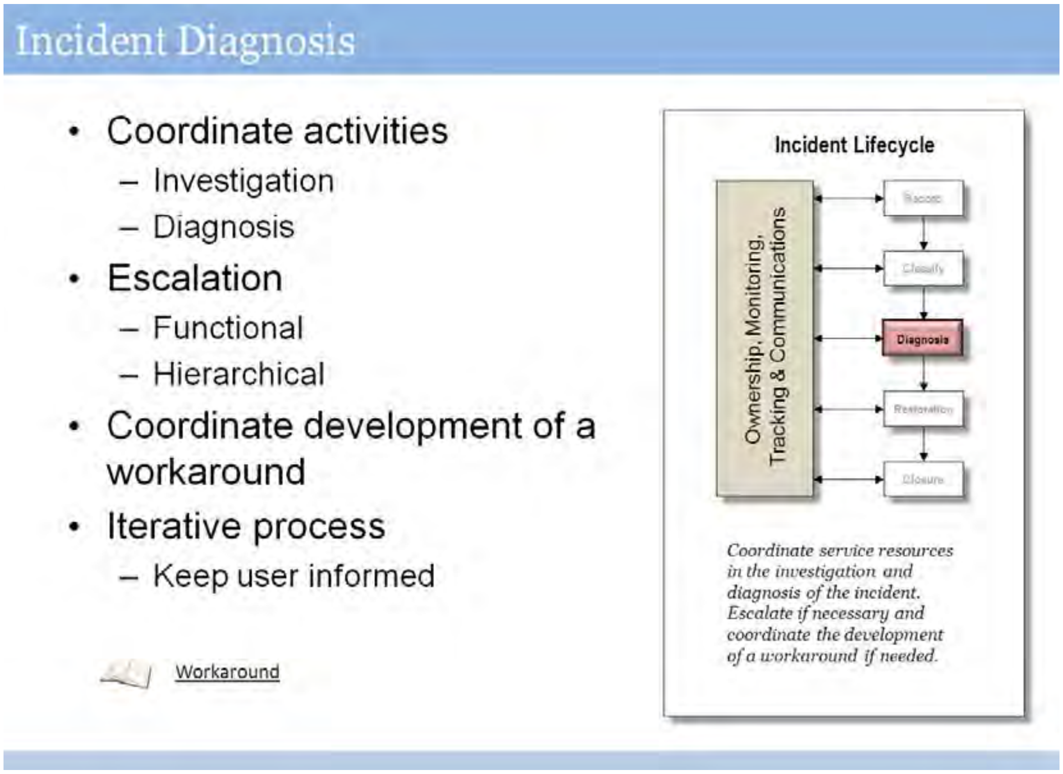
Priority

Priority is a category used to identify the relative importance of an Incident, Problem or Change. Priority is based on impact and urgency and is used to identify required times for actions to be taken.

Business Impact - Business impact is a measure of the business criticality of an Incident. Normally, higher business impact yields higher priority; however, this is not always the case

Business Urgency - Business urgency is a measure of how quickly the Incident needs to be resolved to avoid business impact.

Priority Assignment - Priority can change as the progress toward an incident's resolution advances. User input and SLA targets factor into the assignment of the incident's Priority. An Incident within SLA limits may reduce the priority while an Incident outside SLA limits may increase the priority. For example, an Incident might involve a single individual who cannot access an application, which seems minor. However, the Incident might have a major impact and require urgency in its resolution if the application impacted is a treasury funds transfer program for a brokerage firm.



Incident Diagnosis

- Coordinate activities
  - Investigation
  - Diagnosis
- Escalation
  - Functional
  - Hierarchical
- Coordinate development of a workaround
- Iterative process
  - Keep user informed

Workaround

Coordinate service resources in the investigation and diagnosis of the incident. Escalate if necessary and coordinate the development of a workaround if needed.

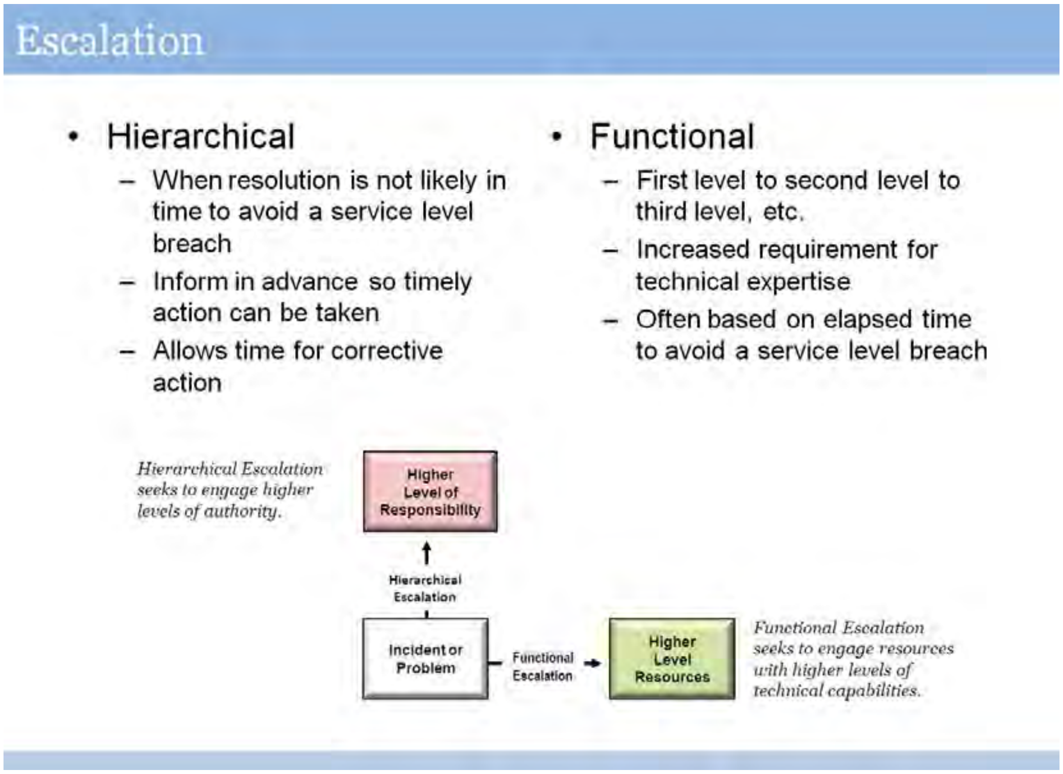
Incident Diagnosis

The goal of Incident Diagnosis is to diagnose and understand the incident and to coordinate the development of a workaround that allows the user to continue business even if this might mean the use of a degraded service. The Incident Management process coordinates the investigation and the diagnosis of the Incident. Diagnosing an Incident is often an iterative process involving different technical support groups and support staff from different vendors.

Depending on the Service Level Agreement (SLA), failure to resolve an Incident within a specified period can initiate the escalation of an Incident. This includes escalating to second- or third-level (or line) support specialists with special skills; for example, developers, architects, or even third-party support staff.

The Incident Management process can coordinate the identification of a workaround for an Incident to get the user working again, even if that means in a degraded capacity. For example, the workaround for the inability to print to a local printer may be printing to a remote printer. Although the users may have to walk a bit farther to get their documents, they can still print until their printer is working again. During the Diagnosis phase, the Service Desk keeps the user informed of the status and progress of the Incident.

> A workaround reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Known Error Records document workarounds for problems, and Incident Records document workarounds for incidents that do not have associated problem records.



Escalation

- Hierarchical
  - When resolution is not likely in time to avoid a service level breach
  - Inform in advance so timely action can be taken
  - Allows time for corrective action
- Functional
  - First level to second level to third level, etc.
  - Increased requirement for technical expertise
  - Often based on elapsed time to avoid a service level breach

Hierarchical Escalation seeks to engage higher levels of authority.

Higher Level of Responsibility

Hierarchical Escalation

Incident or Problem

Functional Escalation

Higher Level Resources

Functional Escalation seeks to engage resources with higher levels of technical capabilities.

Escalation

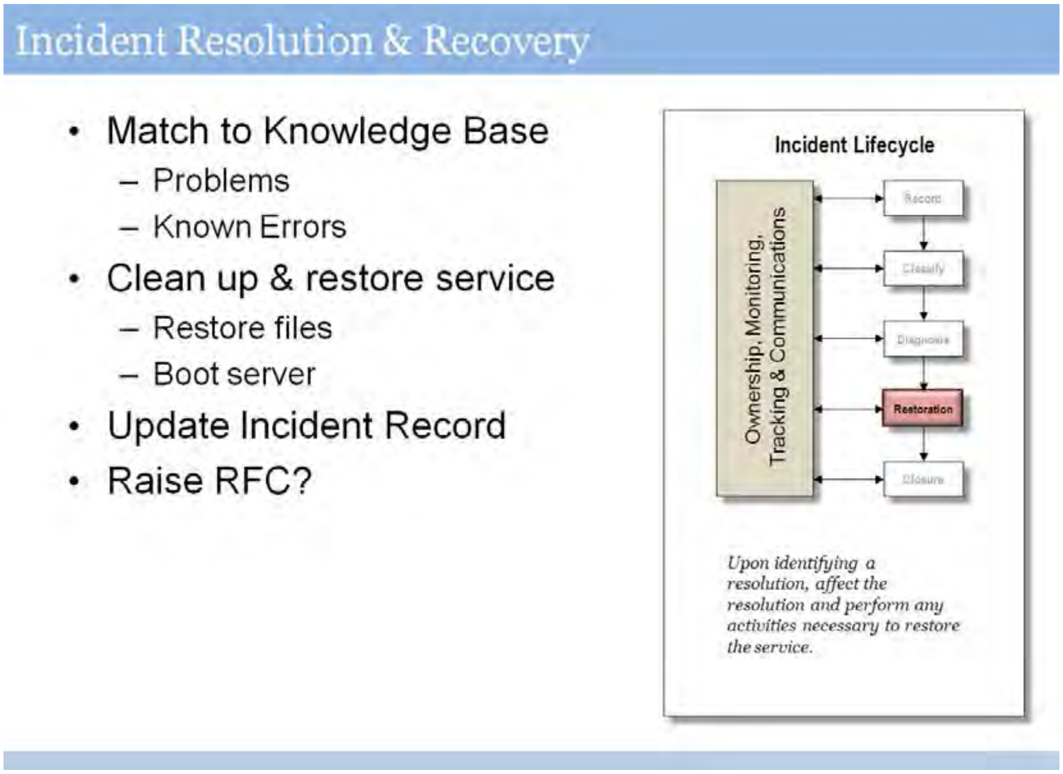
Escalation - Escalation takes place when information about requesting action upon an Incident, Problem or Change is passed to more senior staff or other specialists.There are two types of escalation: functional and hierarchical. Escalation can be Functional (requires higher-level support), Hierarchical (requires higher-level management visibility) or both.

Reasons for escalation include:

- Incidents exceeding SLA allowed downtime
- Increased and unforeseen impact, dimension, or scope of outage
- Notification that timing is such that a critical business activity that is outside the scope of the defined priority matrix may be in jeopardy

Functional Escalation - Functional Escalation represents the requirement for additional functional or technical expertise. This type of escalation takes into account the SLA and duration of the Incident with the intent to avoid potential service level breaches; for example, passing the Incident from first-level support to second-level (or line) support.

Hierarchical Escalation - Hierarchical Escalation invokes the management chain-of-command when the resolution of the Incident is not likely to occur in time to avoid a service level breach. When used in advance of the service level breach, additional resources and timely actions can prevent service outages; for example, alerting senior management to ensure resource commitment occurs.



Incident Resolution & Recovery

- Match to Knowledge Base
  - Problems
  - Known Errors
- Clean up & restore service
  - Restore files
  - Boot server
- Update Incident Record
- Raise RFC?

Incident Lifecycle

Upon identifying a resolution, affect the resolution and perform any activities necessary to restore the service.

Incident Resolution & Recovery

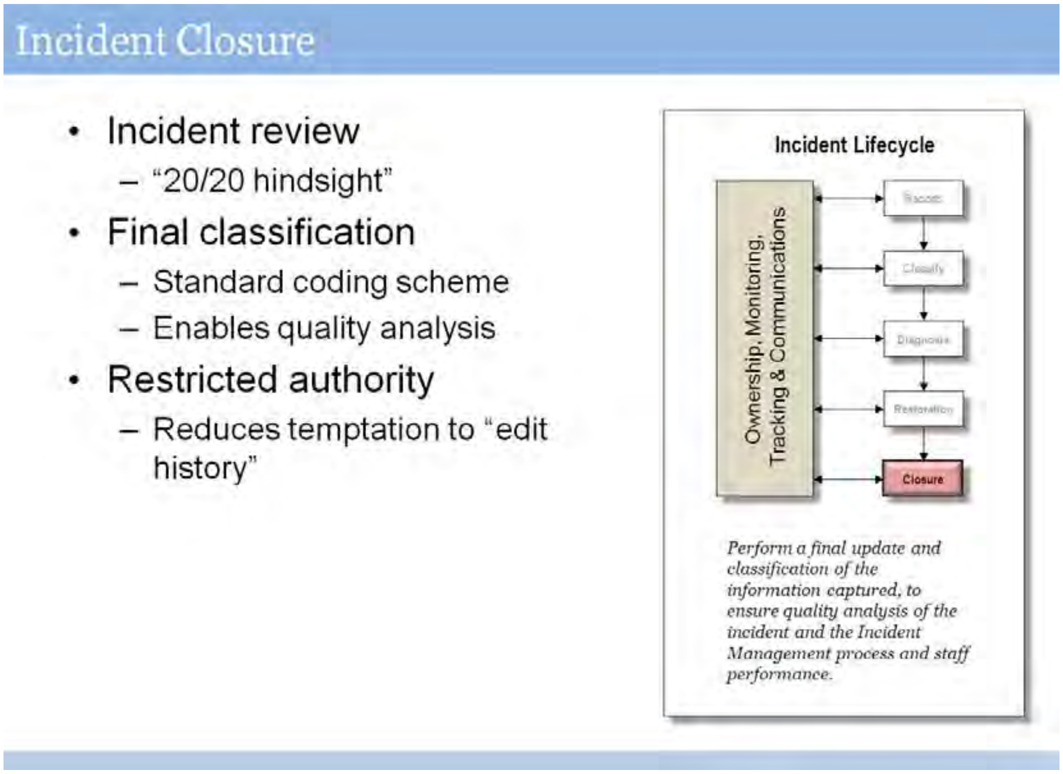
The Incident Management process owns the responsibility for restoration (repair & recovery) for simple or routine incidents. At times, it may be necessary to pass responsibility to other groups that perform Problem Management activities.

It always involves Problem Management when it is not clear which support group should investigate or resolve an Incident. In all cases, Incident Management updates the Incident Record as the Incident progresses and keeps the user informed of the status.

Resolution of the Incident results in the restoration of service to the user through recovery of a repaired Configuration Item (CI). The resolution of the Incident may encompass the application of a workaround determined through Incident matching, or involve other processes such as Problem and Change Management

Repair, or the break/fix of the failed CI, may still leave the service unavailable. For example, replacing a failed hard drive leaves a workstation unavailable until the support team reinstalls the operating system and the user's data. Depending on the scope of the failure, it may be necessary to raise a Request for Change (RFC) before making the repair.

Following repair, Recovery brings the failed CI to its last recoverable state. This includes any required testing, final adjustments or configuration. Examples include restoring files and rebooting. Recovery also includes a step by the Service Desk to notify the user of the restoration. Following Recovery, service Restoration occurs when the user indicates the service is acceptable, and he is able to resume work.



Incident Closure

- Incident review
  - "20/20 hindsight"
- Final classification
  - Standard coding scheme
  - Enables quality analysis
- Restricted authority
  - Reduces temptation to "edit history"

Incident Lifecycle

Perform a final update and classification of the information captured, to ensure quality analysis of the incident and the Incident Management process and staff performance.

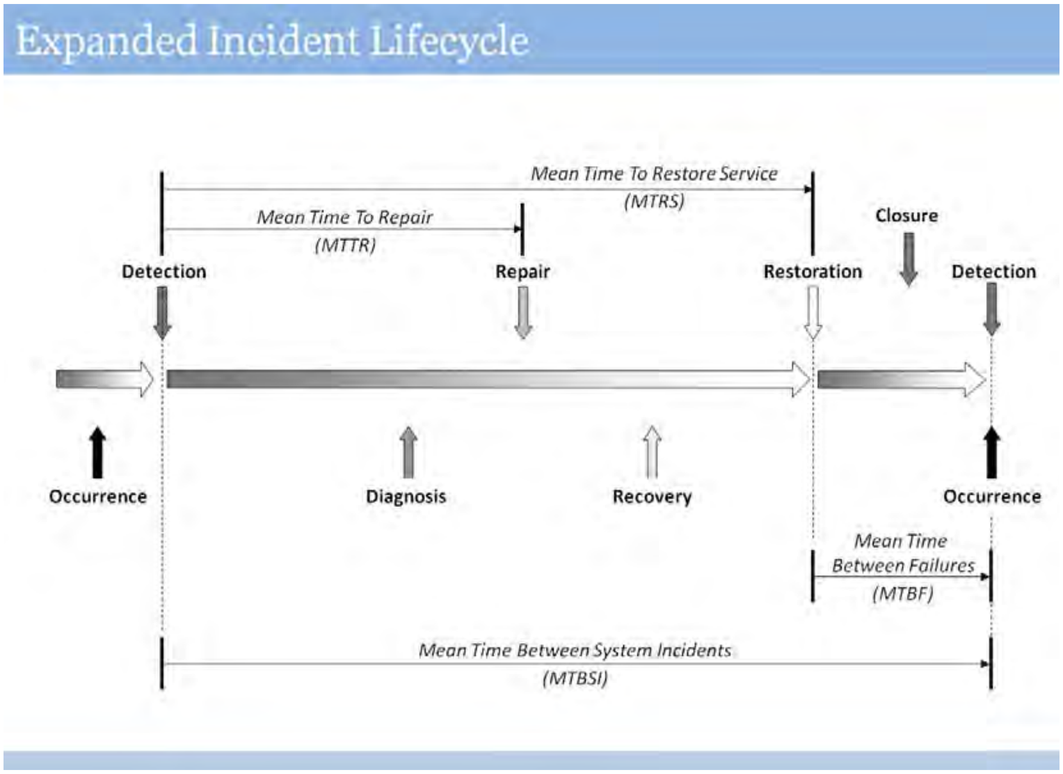
Incident Closure

The Incident Closure Activity ensures constant and accurate updating and closure of an Incident.

After restoring the IT service, Incident Management staff review the Incident to establish its final classification. This takes advantage of "20-20 hindsight" and allows the reviewer, using a standard coding scheme, to accurately record information about the Incident.

Such efforts at the end of the Incident Lifecycle enable the Incident Management process to provide the information necessary to do quality analysis. Final classification also helps ensure accurate matching of new Incidents in the future.

The final step of Incident Closure entails a detailed review of the Incident, the steps taken to restore the IT service, refinement of the data necessary to close the Incident, and agreeing with the originator of the Incident that it is satisfactorily resolved.To reduce the temptation for first-line staff to "re-write history," Service Desk supervisory or senior personnel normally perform this activity.



Expanded Incident Lifecycle

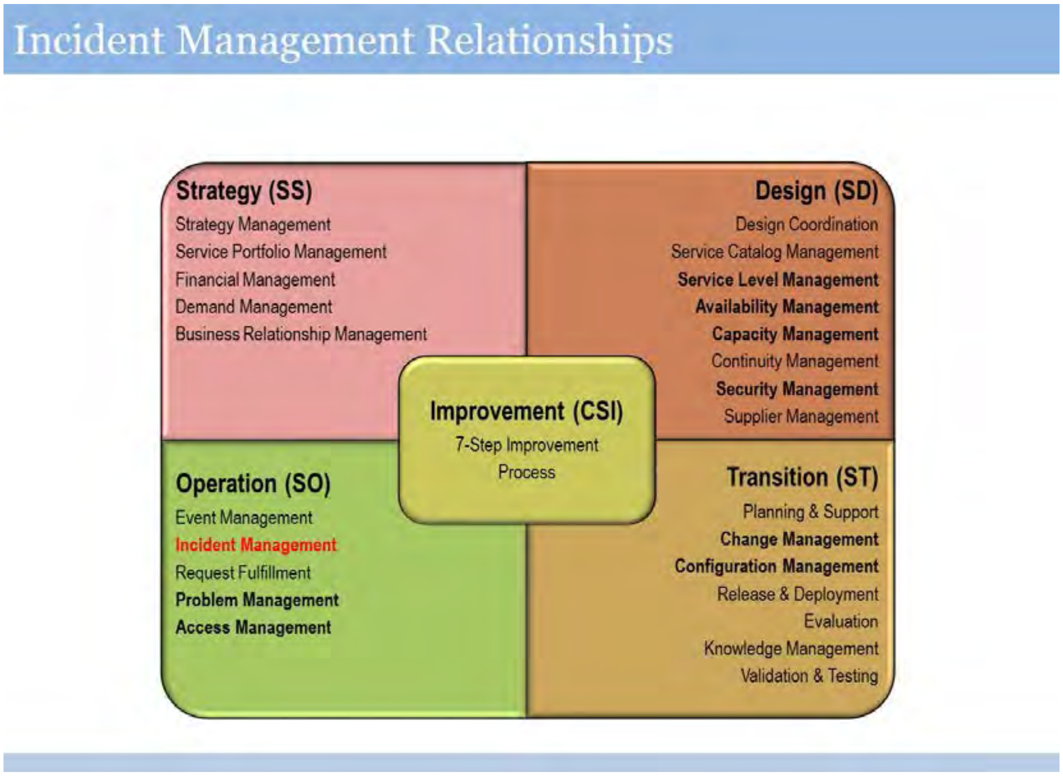
Expanded Incident Lifecycle

The Expanded Incident Lifecycle models the progression of activities between the occurrence of an Incident and the restoration of service.

- **Detection –** When a user or an automated system detects an error with a Configuration Item (CI). There may be a time lag between the incident and its detection.
- **Diagnosis –** Staff members categorize the Incident, and match it to previous Incidents, Problems and Known Errors. If there are no matches, diagnosis activities should start.
- **Repair –**Repair may require the involvement of Change Management. After the CI is repaired, it may still be unavailable to the user until recovery activities take place.
- **Recovery –** Recovery activities, such as required testing, adjustments, etc.
- **Restoration –** Service restoration occurs when the service is available to the user, the user has accepted the service, and the user resumes work.

Metrics– Management metrics associated with Incident resolution:

- **MTTR (Mean Time to Repair) –** mean elapsed time between detection and repair
- **MTRS (Mean Time to Restore Service) –** mean elapsed time between detection and restoration
- **MTBF (Mean Time Between Failures) –** mean elapsed time between restoration and detection
- **MTBSI (Mean Time Between System Incidents) –** average elapsed time between incidents



Incident Management Relationships

Strategy (SS)
Strategy Management
Service Portfolio Management
Financial Management
Demand Management
Business Relationship Management

Design (SD)
Design Coordination
Service Catalog Management
Service Level Management
Availability Management
Capacity Management
Continuity Management
Security Management
Supplier Management

Improvement (CSI)
7-Step Improvement Process

Operation (SO)
Event Management
Incident Management
Request Fulfillment
Problem Management
Access Management

Transition (ST)
Planning & Support
Change Management
Configuration Management
Release & Deployment
Evaluation
Knowledge Management
Validation & Testing

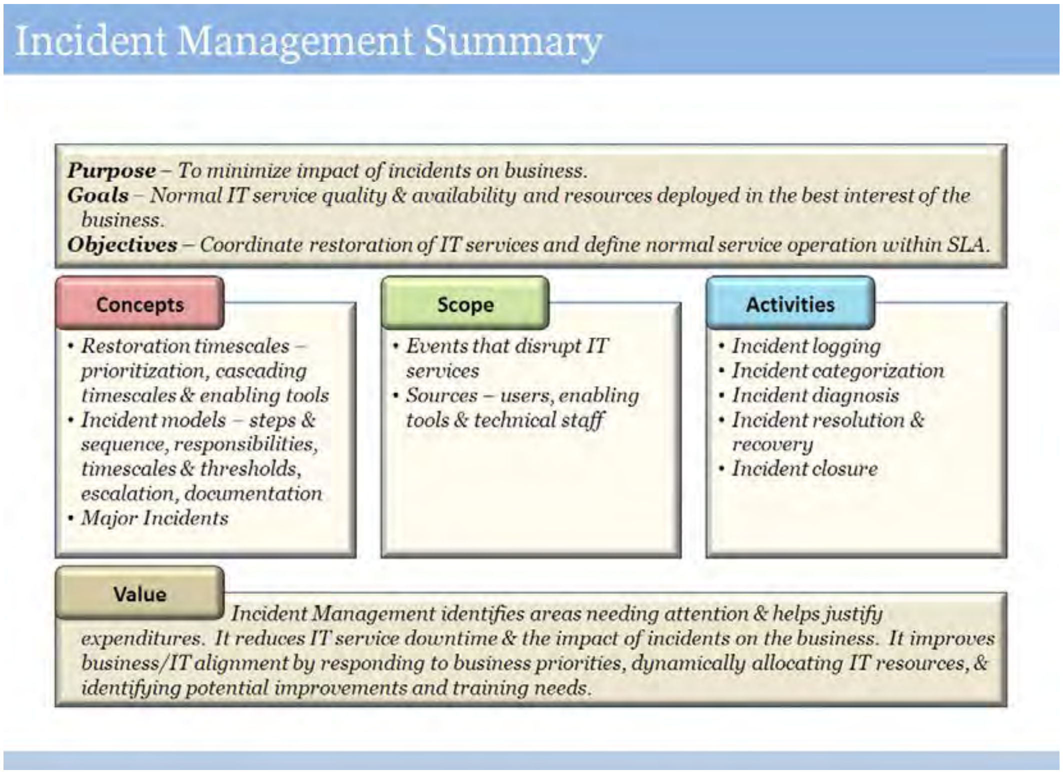
Incident Management Relationships

Incident Management shares relationships with several other processes in the IT Service Lifecycle.

Within the Service Operation stage, the Service Desk function normally owns the Incident Management process. Event Management may notify Incident Management of a disruption to an IT Service, which triggers the Incident Lifecycle. Incidents are an input to the Problem Management process and may trigger the creation of a Problem record. Incident Management should also raise an Incident when there is an unauthorized access attempt or a security breach.

The Incident Management process may raise (initiate) a Request for Change (RFC) if its restoration activity uncovers a defect to the infrastructure that requires a change. Information from the Service Asset & Configuration Management processes often facilitates the investigation and diagnosis of the incident.

The Incident Management process references targets established within Service Level Agreements to help define the Incident timescale. Incident data provides information on unavailability events to both Availability and Capacity Management. In addition, the Incident Management process may utilize Service Design information and staff in the restoration of an IT Service and any capacity-related disruption.



Incident Management Summary

Purpose *– To minimize impact of incidents on business.*
Goals *– Normal IT service quality & availability and resources deployed in the best interest of the business.*
Objectives *– Coordinate restoration of IT services and define normal service operation within SLA.*

Concepts

- *Restoration timescales – prioritization, cascading timescales & enabling tools*
- *Incident models – steps & sequence, responsibilities, timescales & thresholds, escalation, documentation*
- *Major Incidents*

Scope

- *Events that disrupt IT services*
- *Sources – users, enabling tools & technical staff*

Activities

- *Incident logging*
- *Incident categorization*
- *Incident diagnosis*
- *Incident resolution & recovery*
- *Incident closure*

Value

Incident Management identifies areas needing attention & helps justify expenditures. It reduces IT service downtime & the impact of incidents on the business. It improves business/IT alignment by responding to business priorities, dynamically allocating IT resources, & identifying potential improvements and training needs.

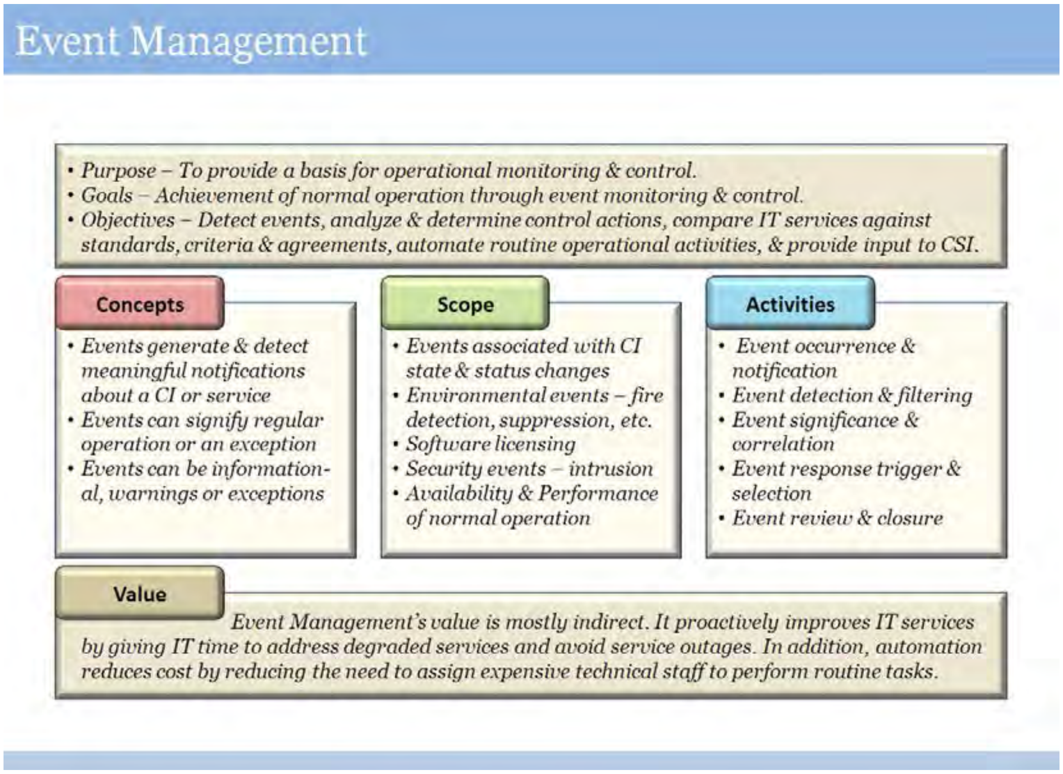
Incident Management Summary

The Incident Management process minimizes the impact an IT Service failure has on the business. It seeks to maintain IT Service quality and availability. It also optimizes the Service Provider's ability to deploy its staff in the best interests of the business.

From the business perspective, Service Operation lies at the heart of realizing IT Service value. The Incident Management process becomes a highly visible area of attention for the business when “things break.” A well-managed Incident Management process sets the stage for, or can provide the justification for, adequate funding of the entire set of Service Operation processes and functions.

Fundamental to the Incident Management process is the idea that not all incidents are equal, and, therefore, they do not require the same level of response in the same time frame. An incident's priority (business impact & urgency) dictates the IT organization's response and the subsequent deployment of its resources.

Incident Management responds to the targets specified within the relevant Service Level Agreements (SLA). Operational Level Agreements (OLA) and Underpinning Contracts (UC) must also support the SLA's restoration targets. Enabling tools can automate this to a certain extent.



Event Management

- *Purpose – To provide a basis for operational monitoring & control.*
- *Goals – Achievement of normal operation through event monitoring & control.*
- *Objectives – Detect events, analyze & determine control actions, compare IT services against standards, criteria & agreements, automate routine operational activities, & provide input to CSI.*

Concepts

- *Events generate & detect meaningful notifications about a CI or service*
- *Events can signify regular operation or an exception*
- *Events can be informational, warnings or exceptions*

Scope

- *Events associated with CI state & status changes*
- *Environmental events – fire detection, suppression, etc.*
- *Software licensing*
- *Security events – intrusion*
- *Availability & Performance of normal operation*

Activities

- *Event occurrence & notification*
- *Event detection & filtering*
- *Event significance & correlation*
- *Event response trigger & selection*
- *Event review & closure*

Value

Event Management's value is mostly indirect. It proactively improves IT services by giving IT time to address degraded services and avoid service outages. In addition, automation reduces cost by reducing the need to assign expensive technical staff to perform routine tasks.

Event Management

Event Management has the responsibility for ensuring the monitoring of all of the events throughout the IT infrastructure. This supports normal on-going operations and enables the detection and escalation exception events. There are three types of events;

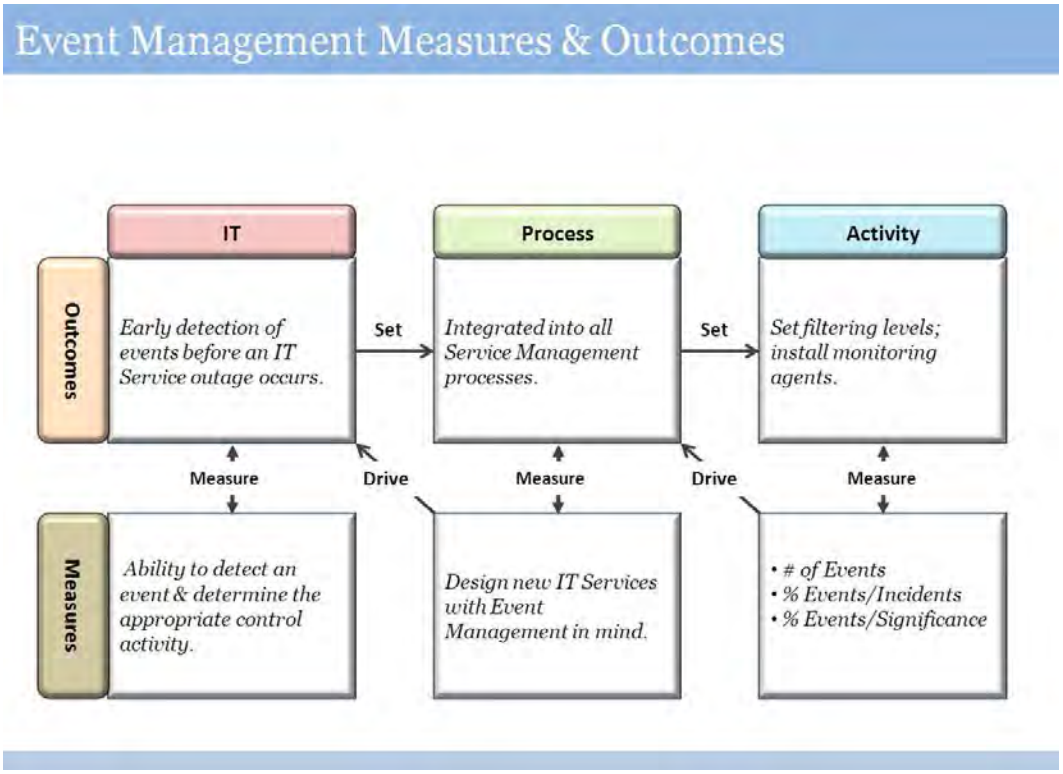
- **Informational** - An event that does not require any action and does not represent an exception
- **Warning** - An event that is generated when a service or devise is approaching a threshold
- **Exception** - An event that means a service or device is currently operating abnormally.

An Event is defined as a change of state that has significance for the management of a Configuration Item or IT service. Sometimes the term is also used to mean an Alert or notification created by any IT service, Configuration Item or monitoring tool. In this context, it is imperative that the Service Level Agreement (SLA) defines what normal service operation is.

In today's IT infrastructure there are a lot of "moving parts." Many events occur during a typical day and the Event Management process helps make sense out of them through:

- Early detection and warning of Incidents
- Exception monitoring
- Integration with Availability & Capacity Management
- Support of automated operations

.



Event Management Measures & Outcomes

	IT	Process	Activity
Outcomes	*Early detection of events before an IT Service outage occurs.*	*Integrated into all Service Management processes.*	*Set filtering levels; install monitoring agents.*
Measures	*Ability to detect an event & determine the appropriate control activity.*	*Design new IT Services with Event Management in mind.*	*• # of Events • % Events/Incidents • % Events/Significance*

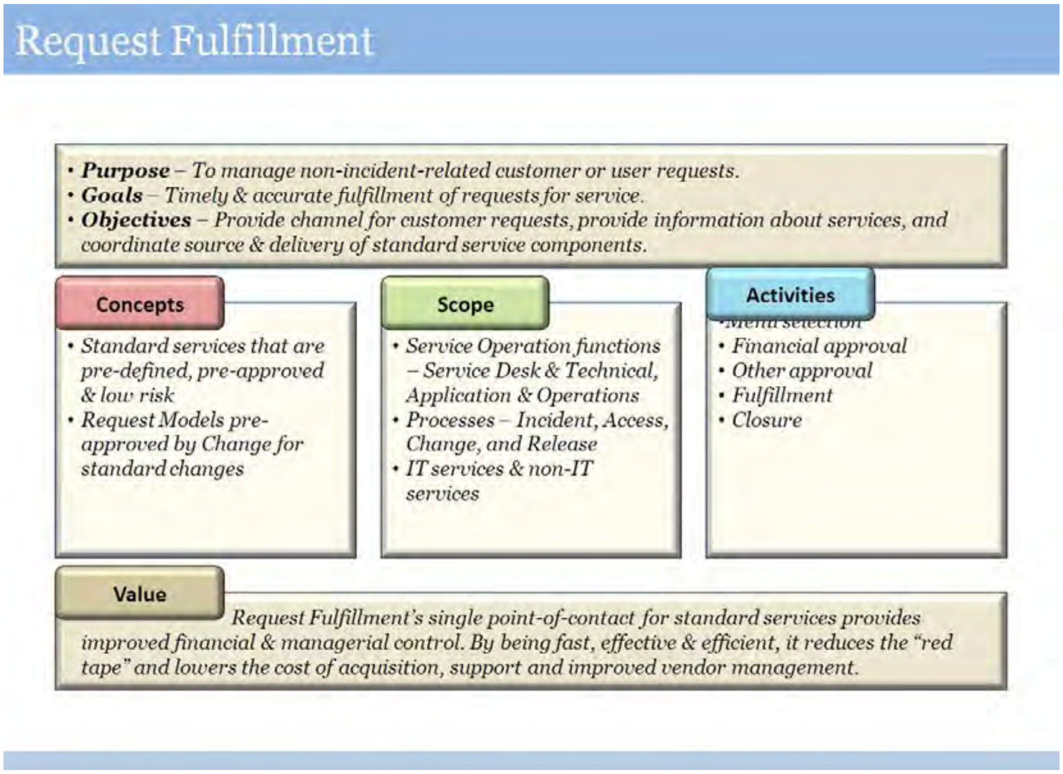
Event Management Measures & Outcomes

Most organizations have a number of sophisticated event monitoring tools that closely follow the health of the infrastructure's components.

Although the monitoring tools can identify every hiccup and discrepancy in a system, they spew forth more information than can be integrated within a short time. The art of successful Event Management is to determine the appropriate levels at which to filter the information coming from these tools.

If you monitor too closely, you will spend many resources investigating Events that turn out to be normal processing events; if you monitor at too high of a level, an Event may turn into an Incident before you have time to correct it.

The key to Event Management is to establish triggers to initiate the investigation of an event and to build Event Management into the specifications of any new or changed services.



Request Fulfillment

- **Purpose** – *To manage non-incident-related customer or user requests.*
- **Goals** – *Timely & accurate fulfillment of requests for service.*
- **Objectives** – *Provide channel for customer requests, provide information about services, and coordinate source & delivery of standard service components.*

Concepts

- *Standard services that are pre-defined, pre-approved & low risk*
- *Request Models pre-approved by Change for standard changes*

Scope

- *Service Operation functions – Service Desk & Technical, Application & Operations*
- *Processes – Incident, Access, Change, and Release*
- *IT services & non-IT services*

Activities

- *Menu selection*
- *Financial approval*
- *Other approval*
- *Fulfillment*
- *Closure*

Value

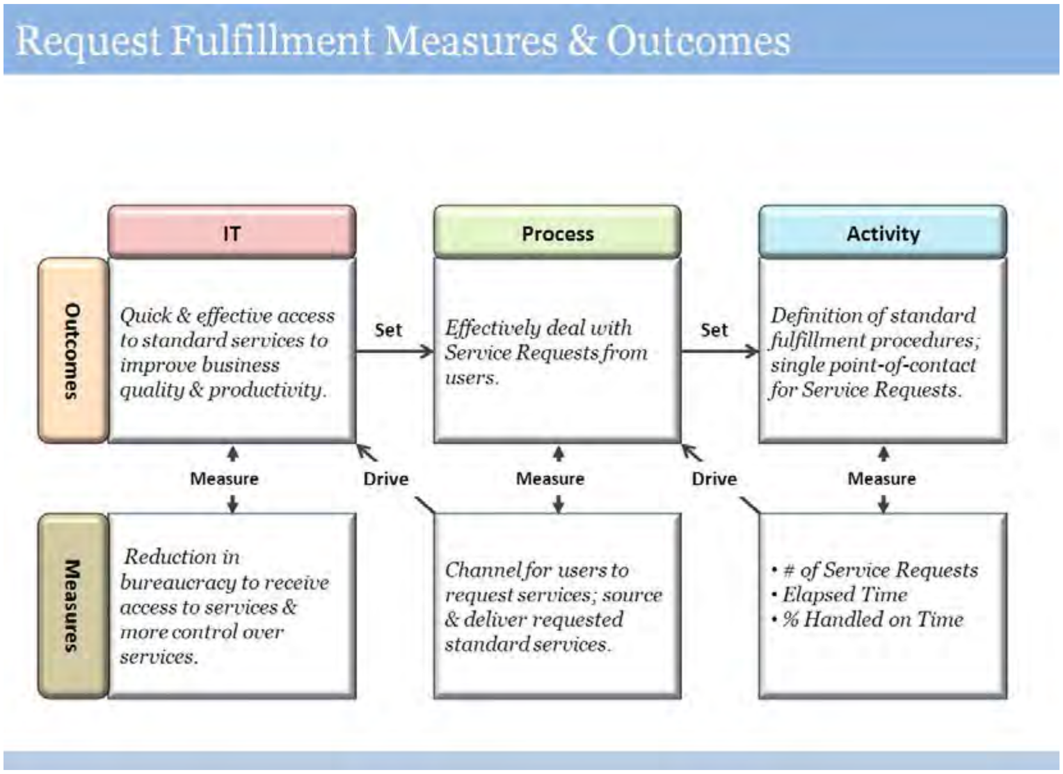
Request Fulfillment's single point-of-contact for standard services provides improved financial & managerial control. By being fast, effective & efficient, it reduces the "red tape" and lowers the cost of acquisition, support and improved vendor management.

Request Fulfillment

A Service Request is defined as a non-incident related request from a user for information, or advice, for a standard change, or for access to an IT service. This includes requests such as a request for a password, or standard change such as the installation of a common off-the-shelf software package.

The Request Fulfillment process provides a conduit for users to request and receive standard services. They can also get information about available services or be told how to request them.

The Service Desk is the normal entry point for users placing requests. However, the actual fulfillment of the request may fall to members of the various technical functional groups responsible for the impacted technology, or with the required skill set to act on the request.



Request Fulfillment Measures & Outcomes

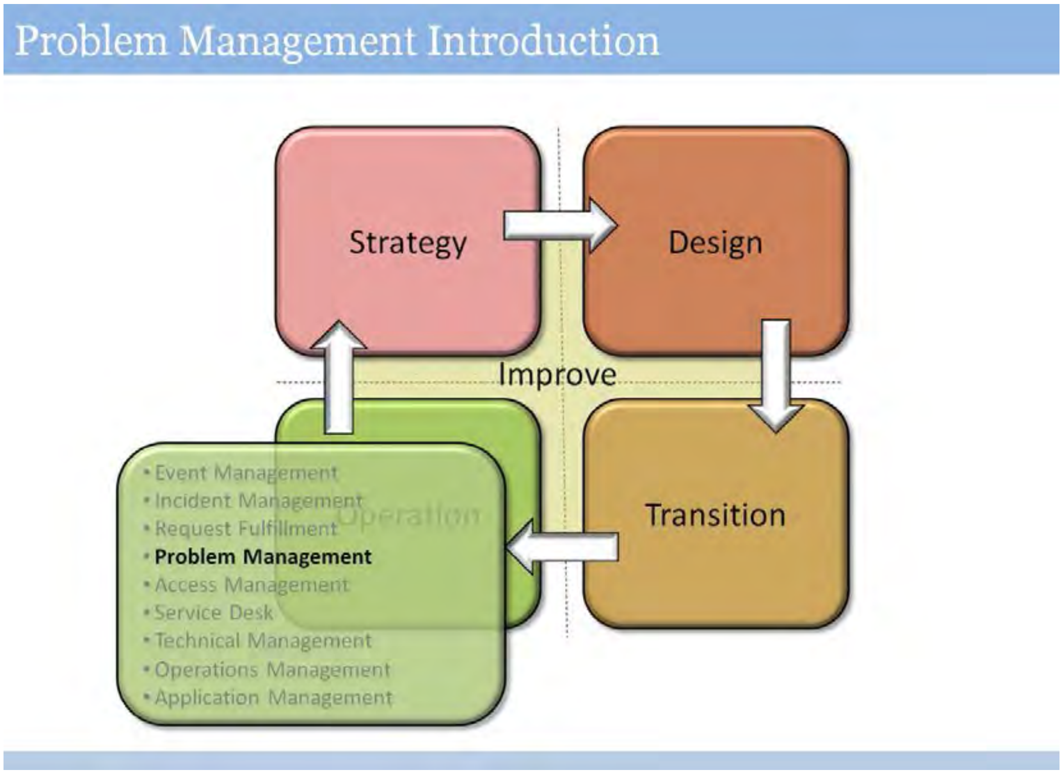
	IT	Process	Activity
Outcomes	*Quick & effective access to standard services to improve business quality & productivity.*	*Effectively deal with Service Requests from users.*	*Definition of standard fulfillment procedures; single point-of-contact for Service Requests.*
Measures	*Reduction in bureaucracy to receive access to services & more control over services.*	*Channel for users to request services; source & deliver requested standard services.*	*• # of Service Requests • Elapsed Time • % Handled on Time*

Request Fulfillment Measures & Outcomes

An IT Service Desk routinely handles many types of Service Requests. The large ones are known as Requests for Change (RFC) and provide input to Service Transition.

However, by far, the most common requests will be small, frequently occurring, inexpensive requests for password resets, copies of documentation, desktop software installations, etc.

The Request Fulfillment process builds the channels and procedures for users to request these standard services. It has a dual objective - to provide quick response to user requests and to avoid congesting and obstructing the Incident and Change Management processes.



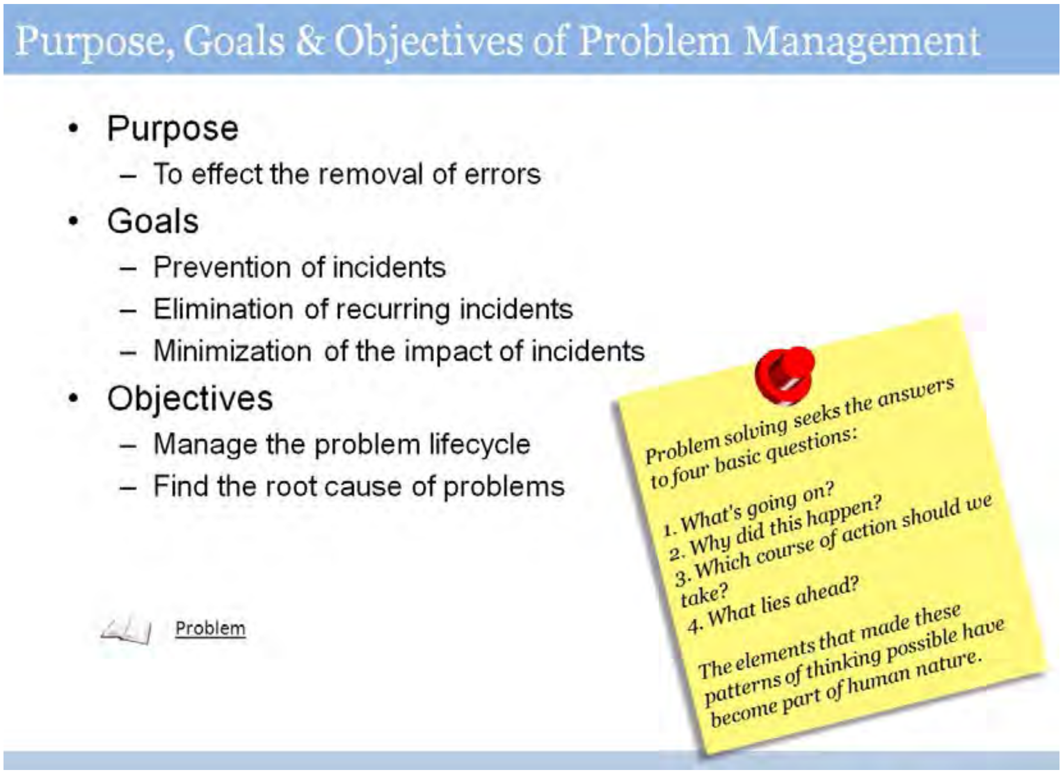
Problem Management Introduction

- Event Management
- Incident Management
- Request Fulfillment
- **Problem Management**
- Access Management
- Service Desk
- Technical Management
- Operations Management
- Application Management

Problem Management Introduction

As one of the processes of the Service Operation phase in the Service Lifecycle, the Problem Management process provides a systematic approach to identifying problems and diagnosing their root causes. Once it diagnoses a problem, Problem Management manages activities from the Known Error stage through to a Request for Change (RFC) and then tracks the Problem through the Change and the Release & Deployment Management processes. It also synchronizes problems between the Development and the Live Environments.

Problem Management activities cover both reactive and proactive aspects of dealing with systemic errors in the infrastructure.



Purpose, Goals & Objectives of Problem Management

- Purpose
  - To effect the removal of errors
- Goals
  - Prevention of incidents
  - Elimination of recurring incidents
  - Minimization of the impact of incidents
- Objectives
  - Manage the problem lifecycle
  - Find the root cause of problems

Problem

Problem solving seeks the answers to four basic questions:

1. What's going on?
2. Why did this happen?
3. Which course of action should we take?
4. What lies ahead?

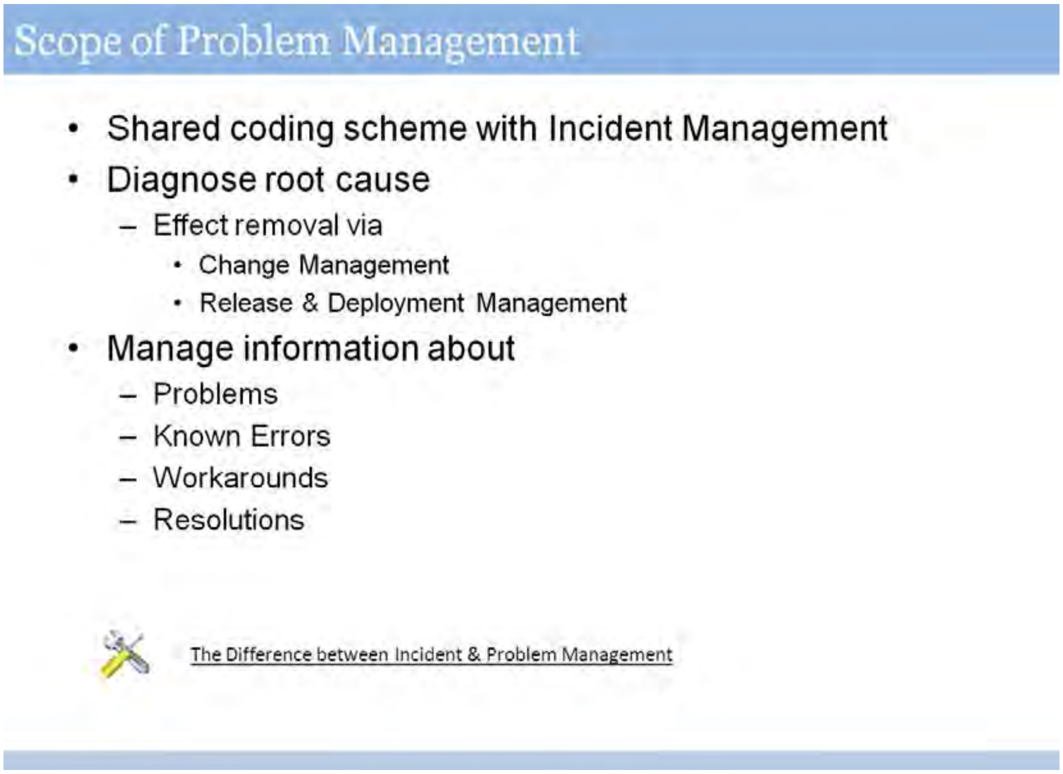
The elements that made these patterns of thinking possible have become part of human nature.

Purpose, Goals & Objectives of Problem Management

Problem Management effects the removal of systemic errors in the infrastructure. It seeks to prevent further incidents by finding and removing the error, thus minimizing the impact of future incidents.

The process oversees the execution of the process' activities and coordinates assets and resources across the departments and functional areas within the Service Provider's organization to seek the root cause of problems.

A Problem is the cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.



Scope of Problem Management

- Shared coding scheme with Incident Management
- Diagnose root cause
  - Effect removal via
    - Change Management
    - Release & Deployment Management
- Manage information about
  - Problems
  - Known Errors
  - Workarounds
  - Resolutions

The Difference between Incident & Problem Management

Scope of Problem Management

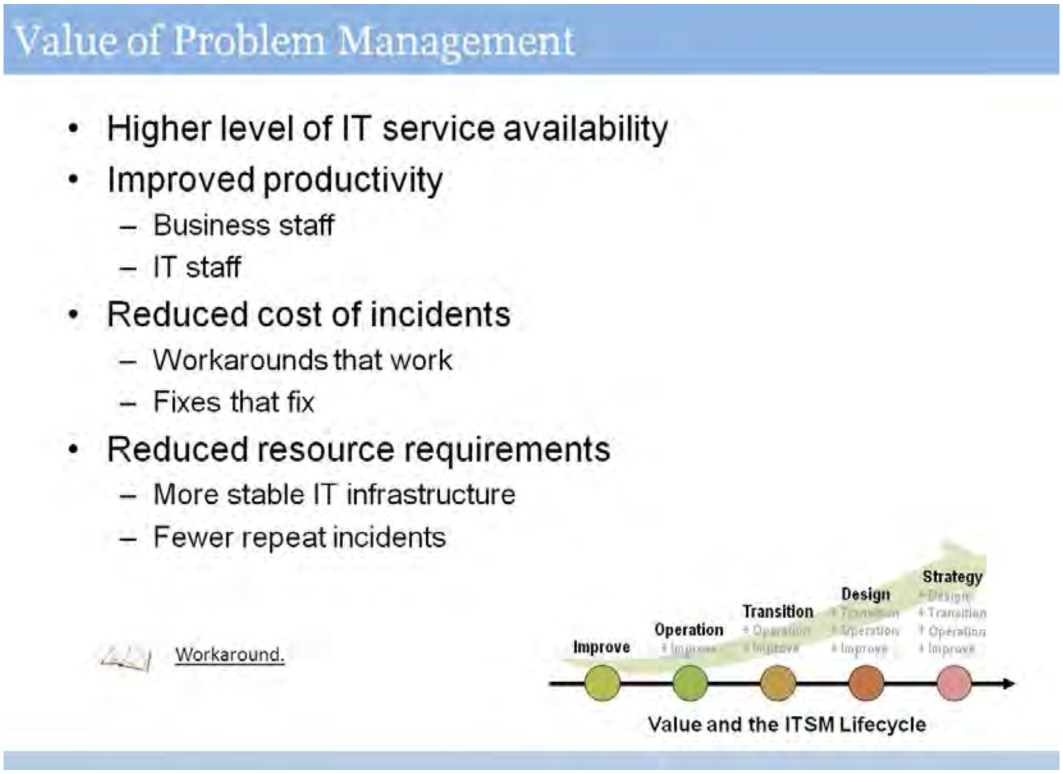
The scope of the Problem Management process extends over the entire Problem lifecycle and includes its interactions with other IT Service Lifecycle domain processes.

Because the Incident and Problem lifecycles closely intertwine with each other, Problem Management shares a common coding scheme for categorizing and prioritizing Incidents and Problems. This significantly improves the likelihood of early Problem detection.

Problem Management's interaction with the Change and the Release & Deployment processes accomplishes the actual removal of a Known Error from the infrastructure. It tracks the Known Error against its progress through the Change and Release Lifecycle.

Information about Incidents, Workarounds, Problems, Known Errors and Resolutions is fundamental to the successful execution of the Problem Management process. It is also key to an IT organization's ability to create and reuse knowledge formulated in the Known Error Database (KEDB), which participates in the overall Service Lifecycle Knowledge Management process.

Incident Management is about restoring services. Problem Management is about finding out what caused the services to fail.Service Providers who fail to understand the distinction between the two will either become really good at "fixing stuff" but not prevent the stuff from breaking, or they will become really good at "finding out" what is causing things to break, but at the expense of the timely restoration of services.



Value of Problem Management

- Higher level of IT service availability
- Improved productivity
  - Business staff
  - IT staff
- Reduced cost of incidents
  - Workarounds that work
  - Fixes that fix
- Reduced resource requirements
  - More stable IT infrastructure
  - Fewer repeat incidents

Workaround.

Value and the ITSM Lifecycle

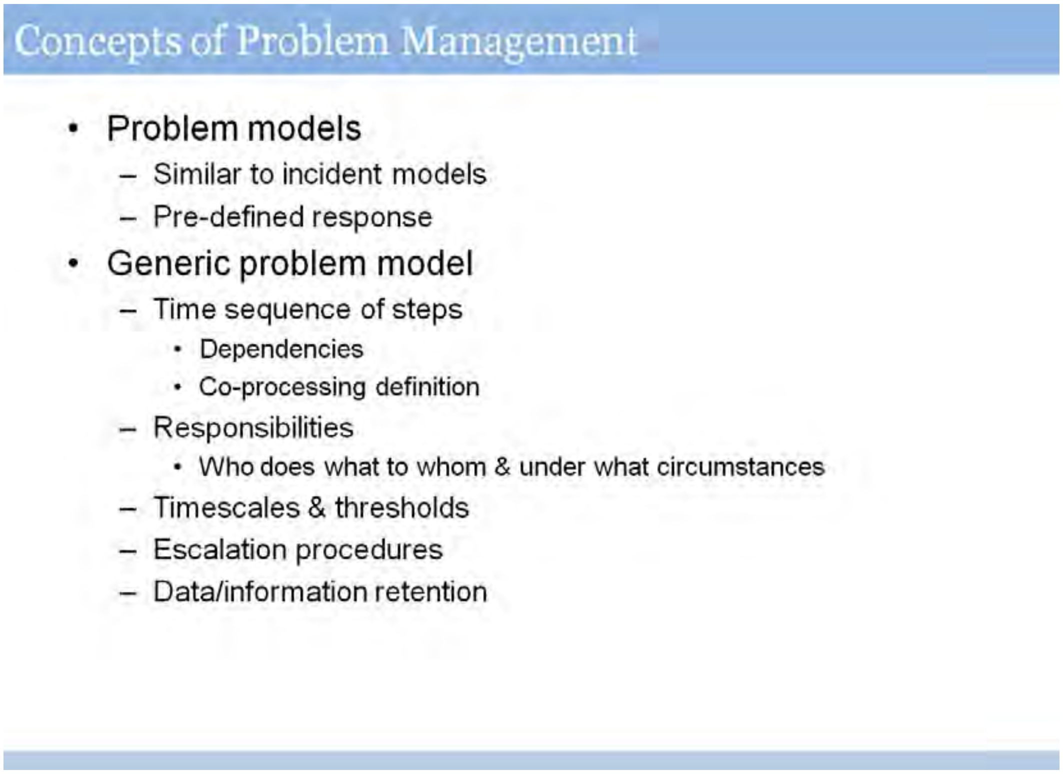
Value of Problem Management

Problem Management creates value for the business in conjunction with the other Service Lifecycle phases and their processes, particularly the Service Desk function and the Incident, Change, Release & Deployment, and Availability Management processes. Through its successful execution, Problem Management creates value in three areas. First, it improves the overall productivity of both business and IT staff by removing systemic errors in the infrastructure. This reduces the overall number and impact of related incidents. The business users experience fewer disruptions that interfere with their work, and IT staff can spend more time on other activities.

Second, fewer Incidents, better workarounds, and fixes that permanently remove errors from the infrastructure reduce the overall cost of Incidents. These cost savings directly relate to business costs and reduction in IT resources consumed in dealing with Incidents.

Third, Problem Management creates real value for the business through the overall reduction in resources consumed in dealing with Incidents. Fewer recurring Incidents free IT staff resources to work on providing new or improved IT Services to the business. The result is a more stable IT infrastructure that provides stable IT Services.

> A workaround reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Known Error records document workarounds for Problems, and Incident records document workarounds for Incidents that do not have an associated Problem record.



Concepts of Problem Management

- Problem models
  - Similar to incident models
  - Pre-defined response
- Generic problem model
  - Time sequence of steps
    - Dependencies
    - Co-processing definition
  - Responsibilities
    - Who does what to whom & under what circumstances
  - Timescales & thresholds
  - Escalation procedures
  - Data/information retention

Concepts of Problem Management

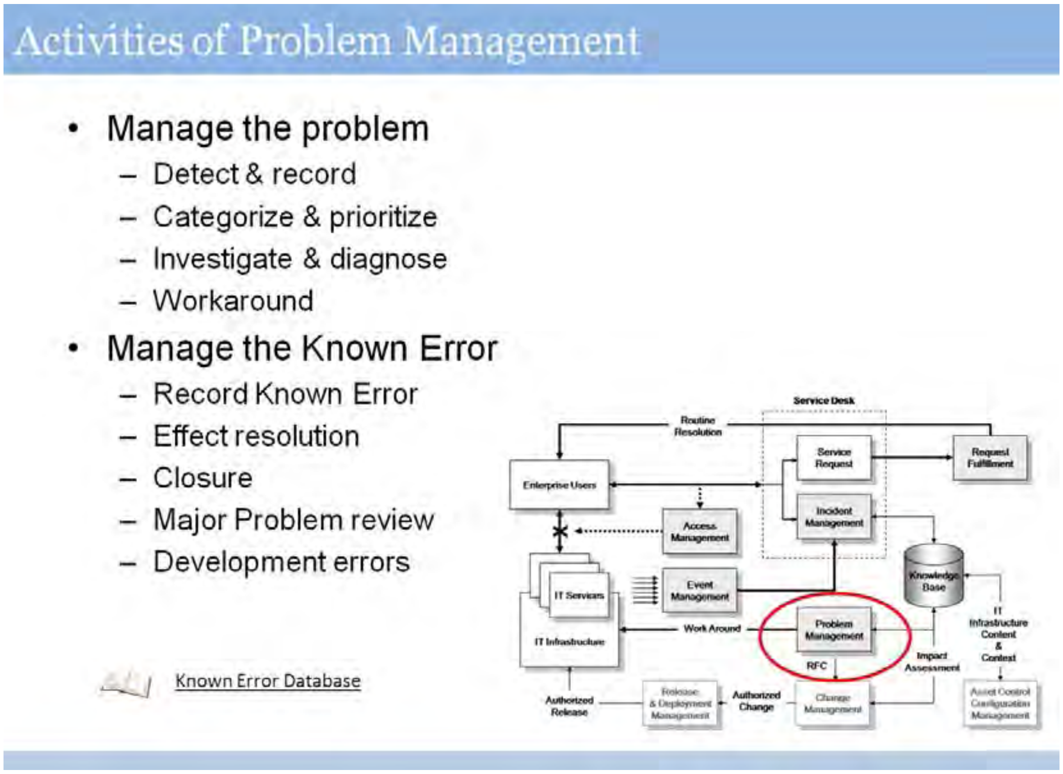
Similar to the Incident Management process, Problem Management deals with managing the IT organization's resources to identify and resolve an abnormal situation. In the case of an Incident, it is the restoration of the impacted IT Service. In the case of a Problem, it is the identification, diagnosis and subsequent removal of the error from the infrastructure.

This commonality lends itself to developing and applying models to aid in the efficient execution of the process. Although not all Problems are the same, the process can create templates or models that provide a pre-defined response to the Problem.

A generic Problem Model lays out the steps to progress a Problem though the Problem Lifecycle. These steps follow a time-sequence, and include any intra- and inter-process dependencies. Clearly defined responsibilities detail who does what, when, and under what circumstances

It defines Problem Lifecycle timescale (timelines), thus allowing for the development of various thresholds for functional and hierarchical escalation. It documents escalation procedures, and measures performance against both time and conformance.

Similar to Incident Management, the Problem Management process is a key contributor to the overall accumulation of organizational knowledge about infrastructure faults, and it plays an important role in the development and retention of the associated information.



Activities of Problem Management

- Manage the problem
  - Detect & record
  - Categorize & prioritize
  - Investigate & diagnose
  - Workaround
- Manage the Known Error
  - Record Known Error
  - Effect resolution
  - Closure
  - Major Problem review
  - Development errors

Known Error Database

Activities of Problem Management

There are two aspects to Problem Management – reactive and proactive.

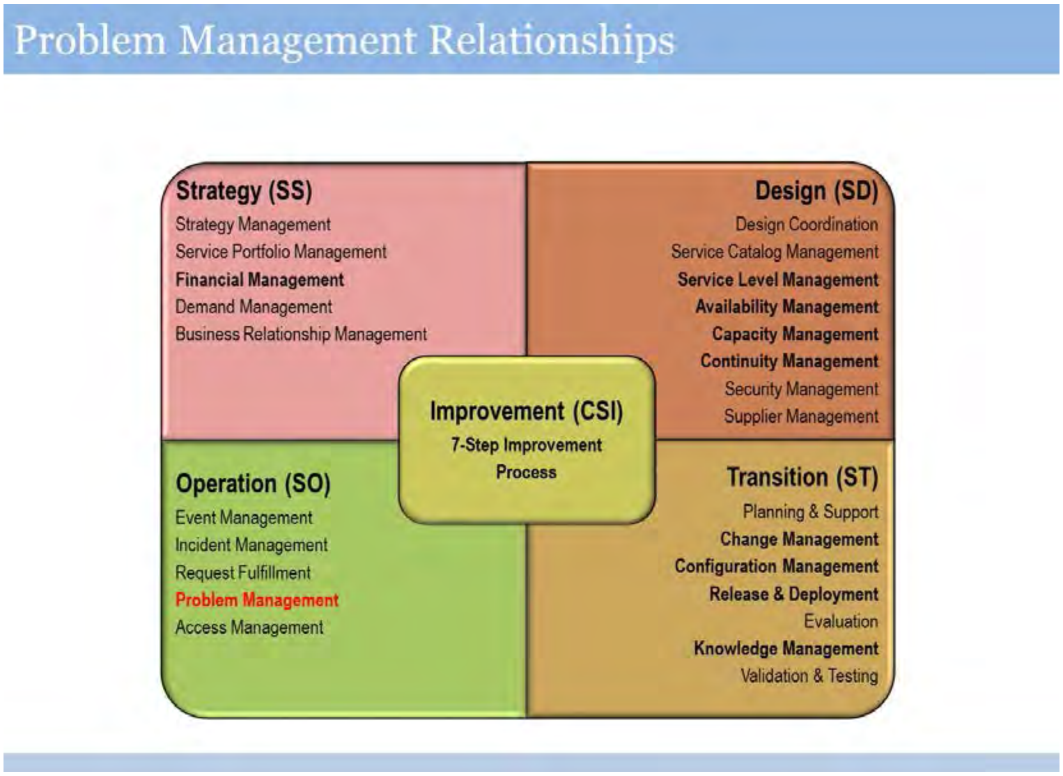
Reactive Problem Management is a two-step process that consists of managing the Problem, followed by managing Known Error.

Managing the Problem involves detecting and recording the Problem, subsequently categorizing and prioritizing it, and, finally, investigating and eventually diagnosing it. It also vets workarounds in conjunction with the Incident Management process.

Managing Known Errors deals with the disposition of each Known Error. It tracks the Known Error through its recording and handoff to the Change and Release & Deployment processes. It closes out the Known Error record upon removal of the error from the infrastructure. It is also conducts Major Problem Reviews and synchronizes the live and development Known Error Databases (KEDB).

Proactive Problem Management essentially follows the Continual Service Improvement (CSI) phase's 7-Step Improvement Process by: (1) baselining the existing service, defining what needs to be measured, defining what can be measured, measuring performance, processing the data into information, analyzing the information, and implementing corrective action.

> The Known Error Database (KEDB) contains all Known Error records. This database is created by Problem Management and used by Incident and Problem Management. The Known Error Database is part of the Service Knowledge Management Systems (SKMS)



Problem Management Relationships

Strategy (SS)
Strategy Management
Service Portfolio Management
Financial Management
Demand Management
Business Relationship Management

Design (SD)
Design Coordination
Service Catalog Management
Service Level Management
Availability Management
Capacity Management
Continuity Management
Security Management
Supplier Management

Improvement (CSI)
7-Step Improvement Process

Operation (SO)
Event Management
Incident Management
Request Fulfillment
Problem Management
Access Management

Transition (ST)
Planning & Support
Change Management
Configuration Management
Release & Deployment
Evaluation
Knowledge Management
Validation & Testing

Problem Management Relationships

Problem Management shares a relationship with several other IT Service Lifecycle processes.

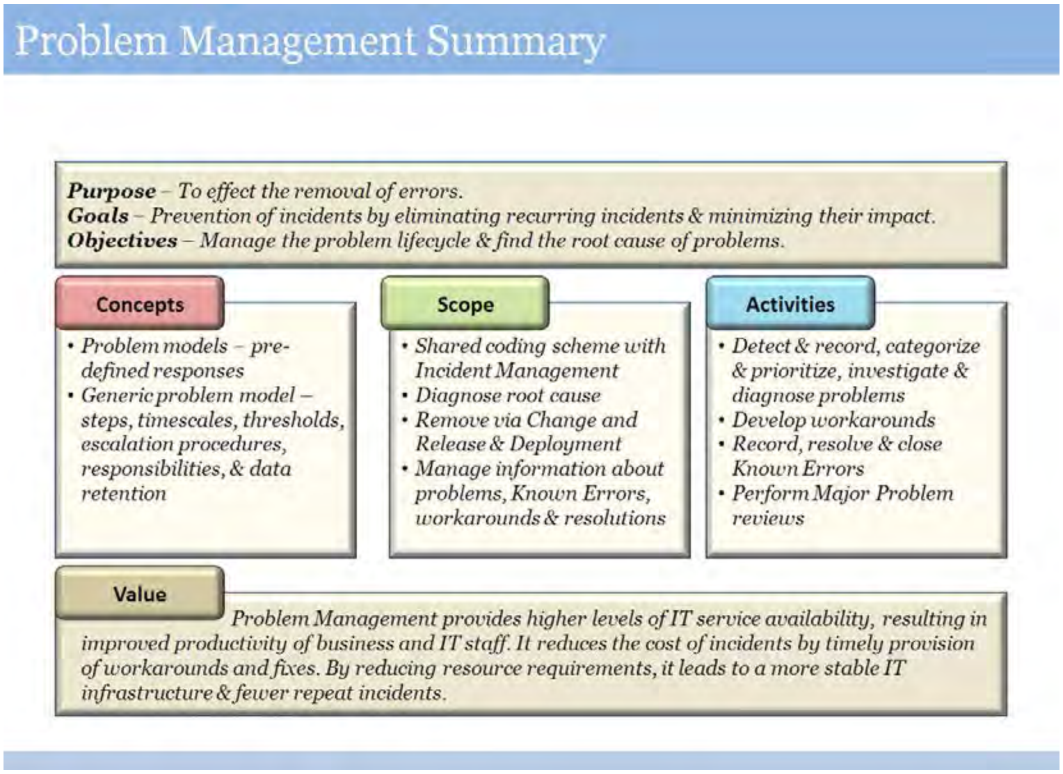
Within the Continual Service Improvement (CSI) phase, Problem Management contributes to the overall improvement of service levels and addresses the need to manage Problems proactively. It also follows CSI's 7-Step Improvement Process for proactive Problem Management.

Along with the Service Desk function and the Incident Management process, Problem Management complements Service Operations's overall effort to stabilize the IT infrastructure and improve the overall quality of service (QoS).

Known Errors that result in the raising of a Request for Change (RFC) involve Service Transition's Change and Release & Deployment processes. Successful removal of an infrastructure error results in the closure of the Known Error and subsequent updating of the Known Error Database (KEDB).

Often Problems require the involvement of Service Design's Availability, Capacity and Continuity Management processes, primarily from the proactive perspective in an attempt to improve the overall quality of service, and to evaluate a problem's impact on continuity of operations.

Service Strategy's Financial Management process provides the necessary information to evaluate the cost impact of proposed resolutions or workarounds. It also gathers information about the cost of the Problem Management process.



Problem Management Summary

Purpose *– To effect the removal of errors.*
Goals *– Prevention of incidents by eliminating recurring incidents & minimizing their impact.*
Objectives *– Manage the problem lifecycle & find the root cause of problems.*

Concepts

- *Problem models – pre-defined responses*
- *Generic problem model – steps, timescales, thresholds, escalation procedures, responsibilities, & data retention*

Scope

- *Shared coding scheme with Incident Management*
- *Diagnose root cause*
- *Remove via Change and Release & Deployment*
- *Manage information about problems, Known Errors, workarounds & resolutions*

Activities

- *Detect & record, categorize & prioritize, investigate & diagnose problems*
- *Develop workarounds*
- *Record, resolve & close Known Errors*
- *Perform Major Problem reviews*

Value

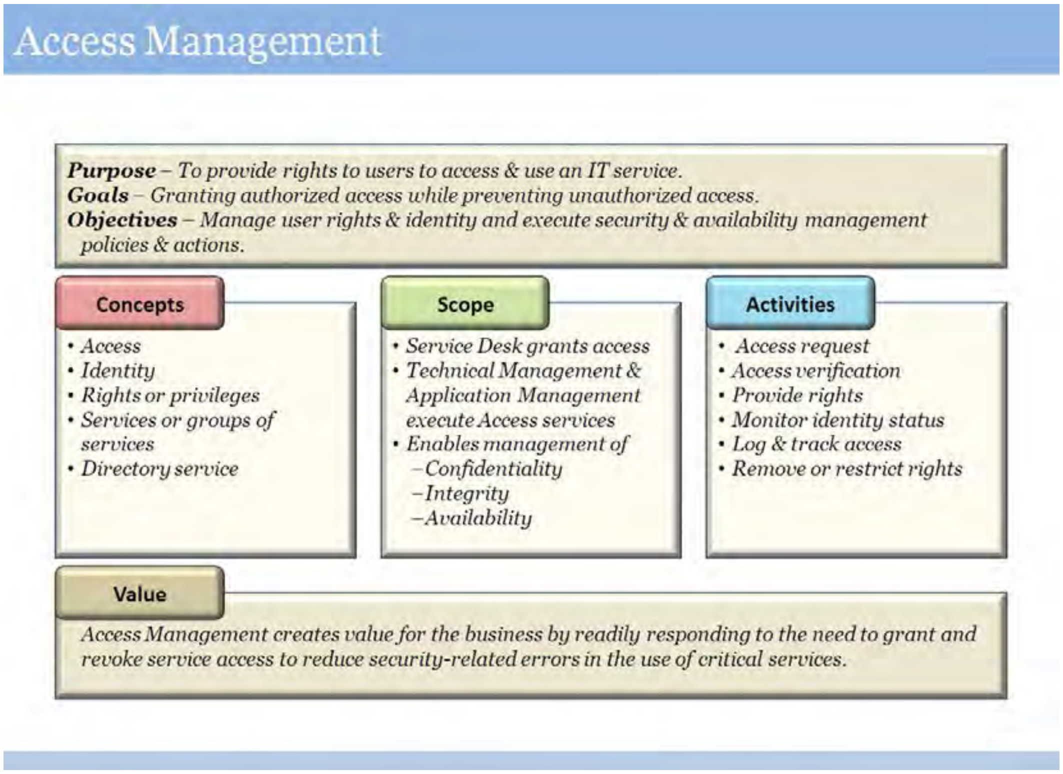
Problem Management provides higher levels of IT service availability, resulting in improved productivity of business and IT staff. It reduces the cost of incidents by timely provision of workarounds and fixes. By reducing resource requirements, it leads to a more stable IT infrastructure & fewer repeat incidents.

Problem Management Summary

Problem Management removes systemic errors to the infrastructure. It prevents further incidents by finding and causing the removal of the error, thus minimizing the impact of future incidents.

Similar to the Incident Management process, Problem Management deals with managing the IT organization's resources in identifying and resolving an abnormal situation. Incident Management focuses on the restoration of the impacted IT Service, and Problem Management focuses on identifying, diagnosing and subsequently removing the error from the infrastructure.

Through the successful execution of the process, it creates value in three areas. It improves the overall productivity of both business and IT staff by removing systemic errors in the infrastructure. Fewer Incidents, better workarounds, and fixes that actually permanently remove errors from the infrastructure reduce the overall cost of Incidents. Finally, it creates real value for the business through the overall reduction in resources consumed in dealing with Incidents.



Access Management

Purpose – *To provide rights to users to access & use an IT service.*
Goals – *Granting authorized access while preventing unauthorized access.*
Objectives – *Manage user rights & identity and execute security & availability management policies & actions.*

Concepts

- *Access*
- *Identity*
- *Rights or privileges*
- *Services or groups of services*
- *Directory service*

Scope

- *Service Desk grants access*
- *Technical Management & Application Management execute Access services*
- *Enables management of*
  - *Confidentiality*
  - *Integrity*
  - *Availability*

Activities

- *Access request*
- *Access verification*
- *Provide rights*
- *Monitor identity status*
- *Log & track access*
- *Remove or restrict rights*

Value

Access Management creates value for the business by readily responding to the need to grant and revoke service access to reduce security-related errors in the use of critical services.

Access Management

Access Management holds responsibility solely for executing the security procedures that the organization's Security policies define.

Requesting Access - Requests to change an access generally emanate from a few, well-defined areas, such as Human Resources, Requests for Change (RFC) or Service Requests. Security policies define who may request access, and Access Management provides the mechanisms to carry out that request.

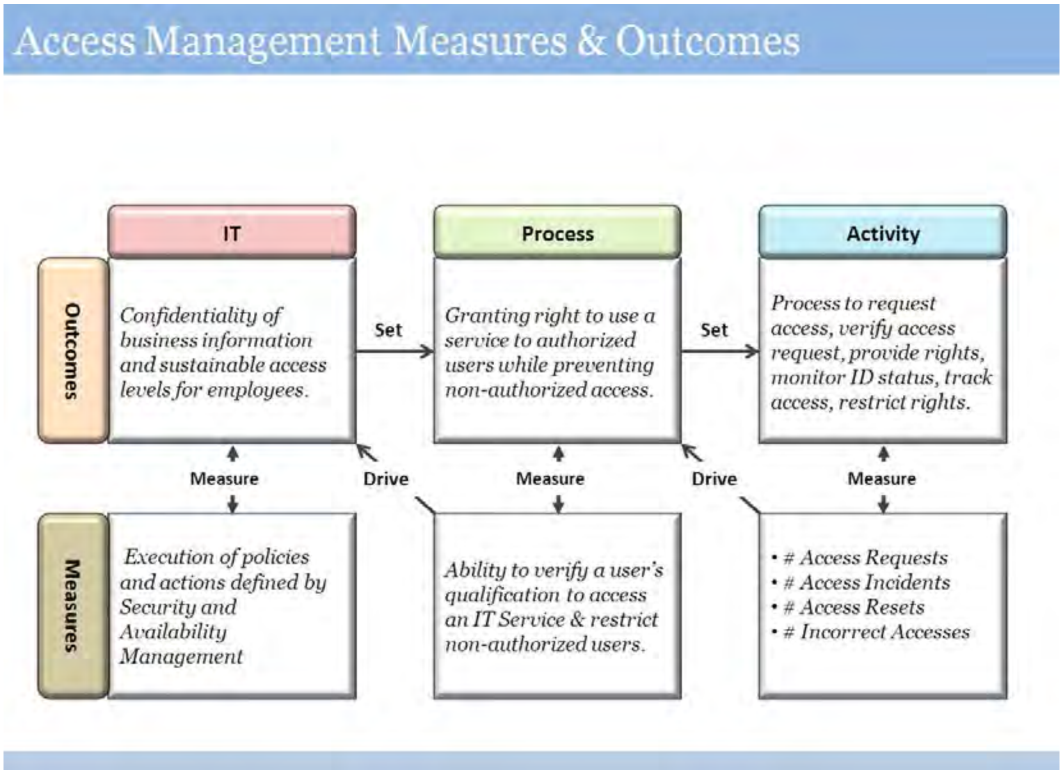
Verification - This activity ensures that the user requesting the access is who he/she says he/she is, and legitimately requires the service. Security policies may define different levels of verifications to access different services.

Providing Rights - The Security policy defines the rights available to an individual, and Access Management grants rights based on this information. It also looks for role conflicts or duplications, and informs the originators of the requests about them.

Monitoring Identity Status - Security policies define trigger events, and Access Management builds ways to capture them. Typical triggers are job changes, promotions or demotions, transfers, resignation or death, retirement, disciplinary actions and dismissals.

Logging & Tracking Access - The Security group develops requirements for monitoring and tracking, and Access Management develops the underlying capabilities. All Technical and Application Management monitoring activities should review Access rights and utilization to ensure that they are being properly used.

Removing or Restricting Rights - Users often change jobs or roles. When a User's status or access requirement changes, Access Management adjusts access rights accordingly.



Access Management Measures & Outcomes

IT

Process

Activity

Outcomes

Confidentiality of business information and sustainable access levels for employees.

Set

Granting right to use a service to authorized users while preventing non-authorized access.

Set

Process to request access, verify access request, provide rights, monitor ID status, track access, restrict rights.

Measure

Drive

Measure

Drive

Measure

Measures

Execution of policies and actions defined by Security and Availability Management

Ability to verify a user's qualification to access an IT Service & restrict non-authorized users.

- # Access Requests
- # Access Incidents
- # Access Resets
- # Incorrect Accesses

Access Management Measures & Outcomes

In the not-so-distant past, IT departments, eager to protect the business against security risks, implemented very stringent security procedures. This created problems that actually voided many of the security efforts as users simply taped their multitude of login names and passwords to their monitor or underneath their desk drawer.

Other processes and parts of the business define who should have access to particular Configuration Items (CI) and services. Access Management executes those policies and actions.

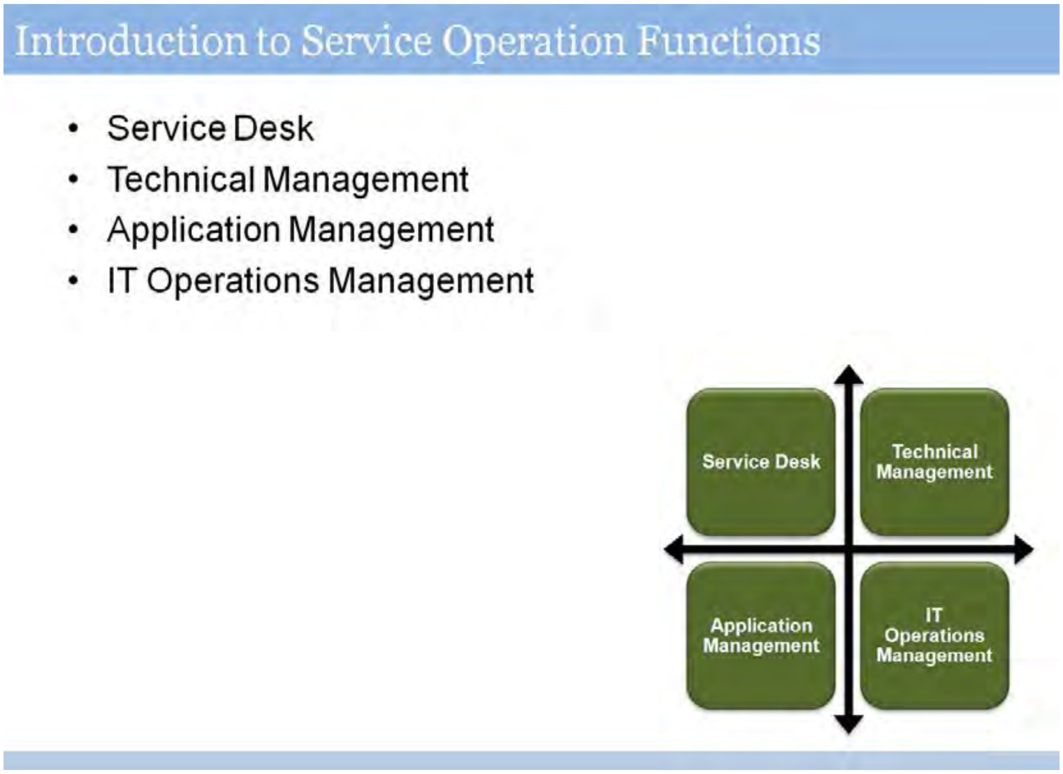
Its goal is to grant the right to use a service to authorized users while preventing non-authorized access to it. Corollary to that is its ability to verify that a user qualifies to access the service.

It can measure its effectiveness by looking at the requests for access and incidents caused by incorrect levels of access. Looking at the number requests for access will indicate whether the Access Management procedures are working properly and efficiently. If the processes are good, it will take very little time to verify the required authorization level of a new user. If the processes are slack, it may take several rounds of collecting more information before IT can grant access.

Likewise, the incorrect levels of access can cause incidents. While incidents caused by users who should not have been granted access immediately come to mind, there can also be incidents caused because a user who should have had access to a service did not have proper access.

Lesson 11

Service Operation Functions



Introduction to Service Operation Functions

- Service Desk
- Technical Management
- Application Management
- IT Operations Management

Service Desk
Technical Management
Application Management
IT Operations Management

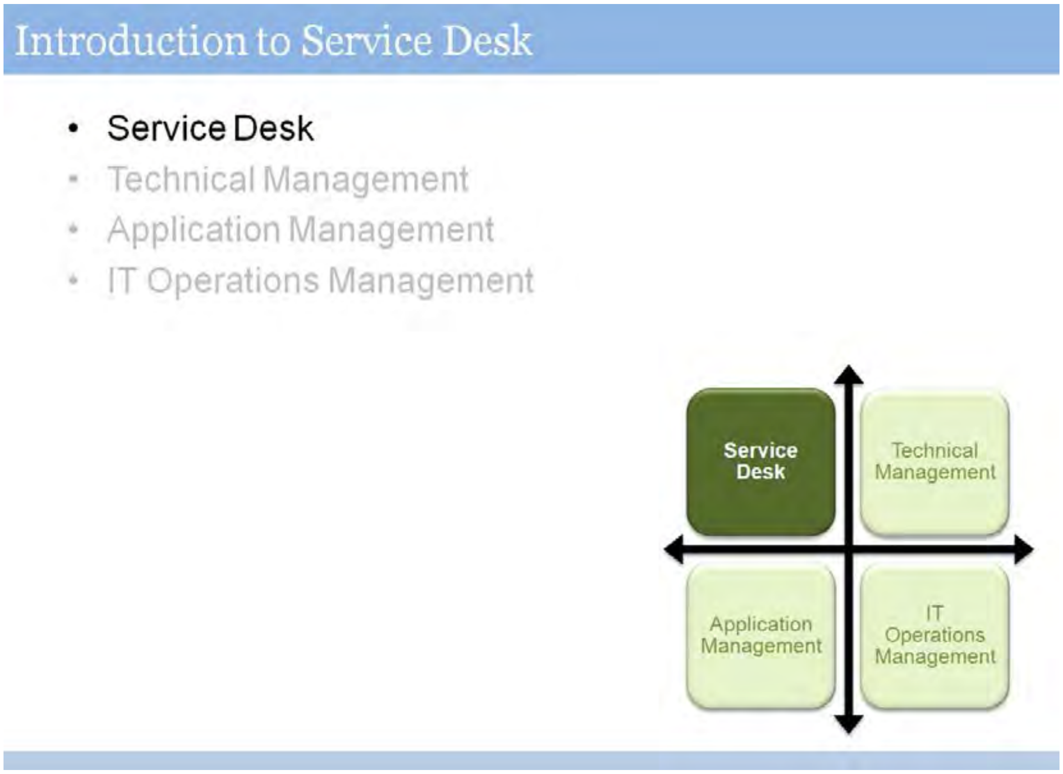
Introduction to Service Operation Functions

ITIL defines a function as a team or group of people and the tools it needs to carry out one or more processes or activities. Large organizations may devote entire departments, teams and groups to performing a single function. Smaller organizations may task a single individual or group with multiple functions.

Many organizations newly exposed to ITIL and to some of its core processes tend to organize functional groups around each process. ITIL, however, emphasizes an environment in which traditional organizational structures easily accommodate ITIL's roles and processes.

ITIL describes four key functions within Service Operation. The Service Desk is the single point of contact between IT and the user community, usually managing the Incident Management and Request Fulfillment processes. Technical Management provides the technical expertise and resources for the overall management of the IT infrastructure.

Application Management manages the enterprise's applications throughout their lifecycle, and IT Operations Management includes the functional groups involved in the day-to-day operational activities. Prior to undertaking any significant restructuring, an organization should consider carefully its size, required technology skill sets, geographical distribution, operating environment, and business objectives.



Introduction to Service Desk

- Service Desk
- Technical Management
- Application Management
- IT Operations Management

Service Desk

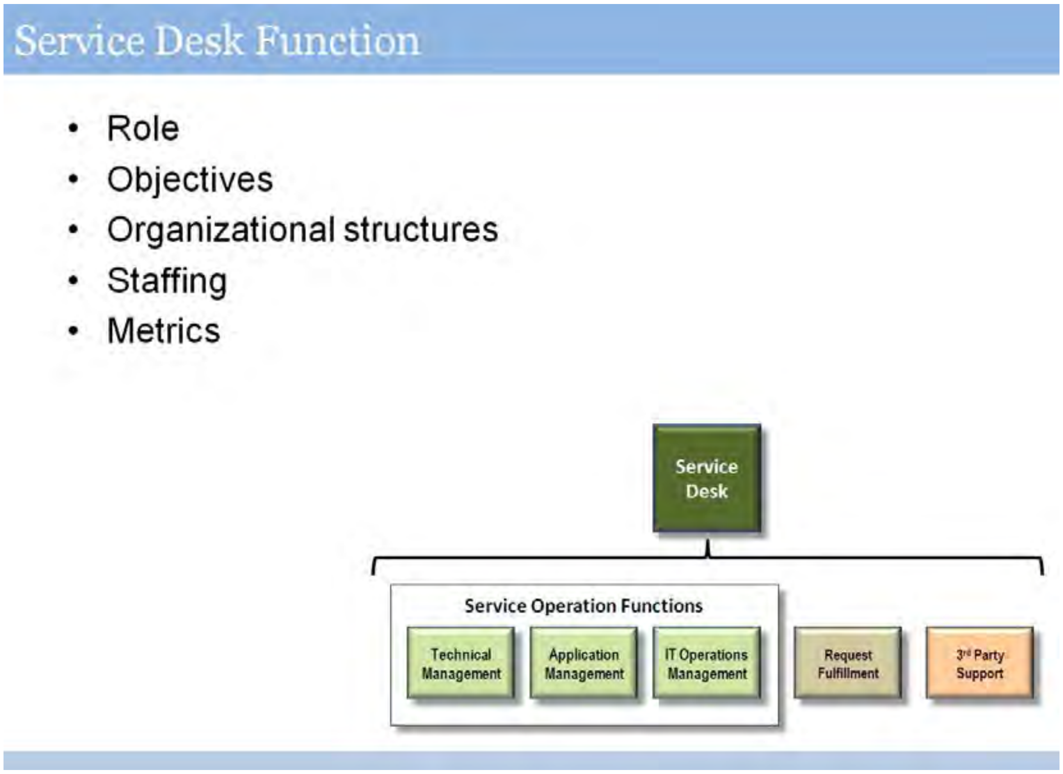
Technical Management

Application Management

IT Operations Management

Introduction to Service Desk

The definition of a function is a team or group of people and the tools they need to carry out one or more processes or activities. As discussed in the ITIL Concepts chapter, many organizations newly exposed to the ITIL and to some of the core processes tend to try to organize their functional groups around the process. In some cases, this is appropriate. In many cases, however, the process extends beyond a single functional group and calls for functional group participation, not a reorganization by functional group.



Service Desk Function

- Role
- Objectives
- Organizational structures
- Staffing
- Metrics

Service Desk

Service Operation Functions

Technical Management

Application Management

IT Operations Management

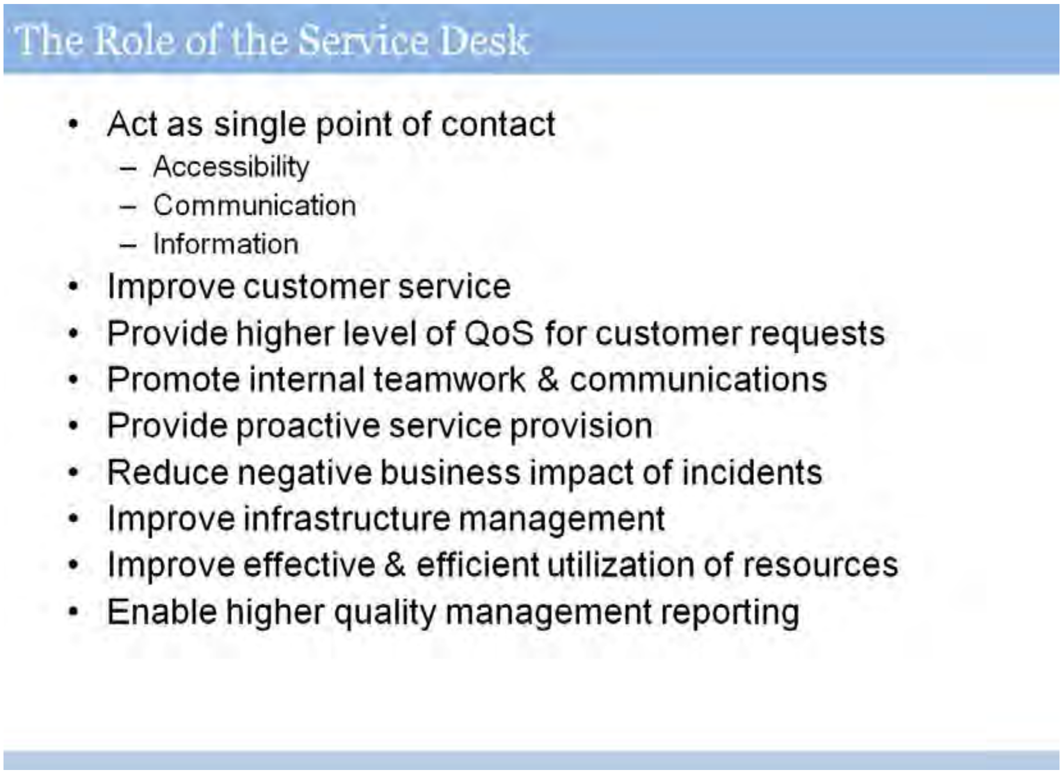
Request Fulfillment

3rd Party Support

Service Desk Function

The Service Desk function plays an important part in the provision and delivery of IT services. It is very often the first contact the users and customers have in their use of IT services. The Service Desk performs first-line support of IT services. While responsible for two of Service Operation's processes, the Service Desk itself is not a process, but a function; i.e., an organizational unit of IT.

Another word often used to refer to the Service Desk is “Help Desk,” but unlike a Help Desk a Service Desks offers a range of services and a more integrated or holistic approach to support by striving to integrate business and customers into the service management infrastructure. A skilled or expert Service Desk extends this concept even further by also providing a contact point between third-party support organizations as well.



The Role of the Service Desk

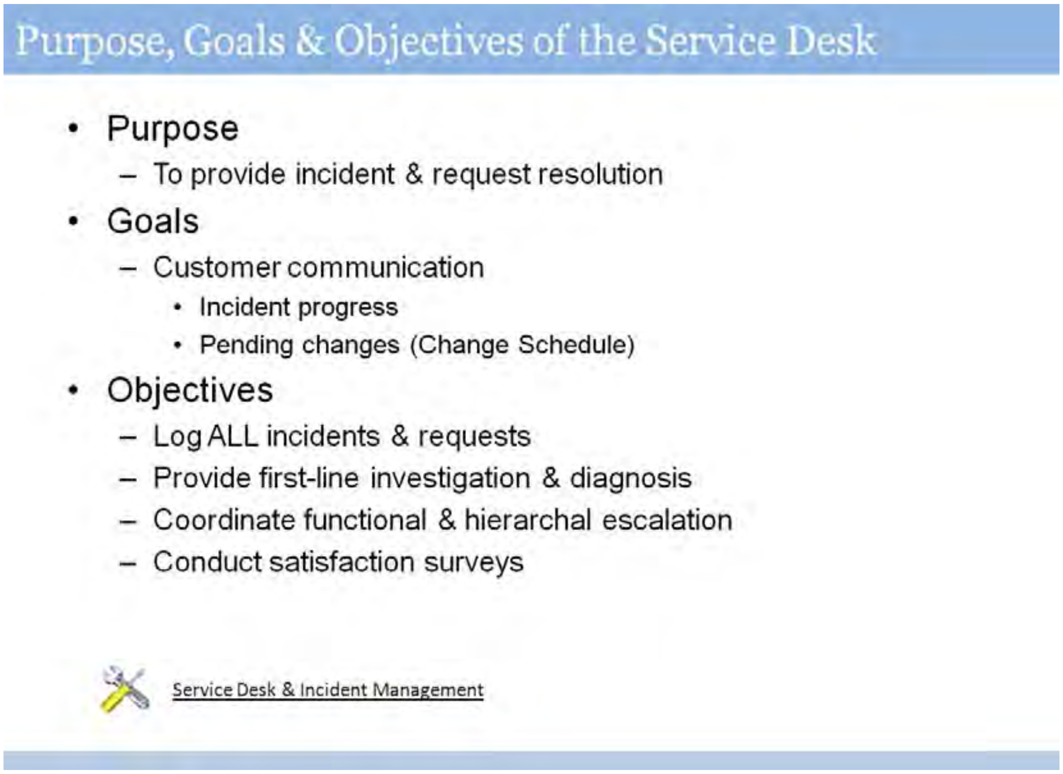
- Act as single point of contact
  - Accessibility
  - Communication
  - Information
- Improve customer service
- Provide higher level of QoS for customer requests
- Promote internal teamwork & communications
- Provide proactive service provision
- Reduce negative business impact of incidents
- Improve infrastructure management
- Improve effective & efficient utilization of resources
- Enable higher quality management reporting

Role of the Service Desk

The Service Desk provides a single point of contact within the IT organization for the users of IT services. As such, it is the conduit for service access, communication between IT and its users, and information about the services themselves. In effect, it acts a “one-stop-shop” for all incidents, questions, comments and requests for service and changes regardless of their reason or source

It is important to draw a clear distinction between the Service Desk's role in an IT organization and its relationship to the Incident Management process. The Service Desk function normally “owns” the Incident Management process. In other words, it fulfills the role of the Incident Management process owner; therefore, it has the responsibility for executing the Incident Management process and is accountable for the outcomes of the process.

Of course, the intent of having a Service Desk is to improve the business user's level of satisfaction with IT services and to help IT achieve a higher level of service quality. It does this through its role as the Incident Management process owner and the coordination of IT resources in the restoration of IT services as well as fulfillment of non-incident related requests. This results in lowering the impact of Incidents, improving overall business and IT resource utilization, and enabling the generation of higher quality management reporting.



Purpose, Goals & Objectives of the Service Desk

- Purpose
  - To provide incident & request resolution
- Goals
  - Customer communication
    - Incident progress
    - Pending changes (Change Schedule)
- Objectives
  - Log ALL incidents & requests
  - Provide first-line investigation & diagnosis
  - Coordinate functional & hierarchal escalation
  - Conduct satisfaction surveys

Service Desk & Incident Management

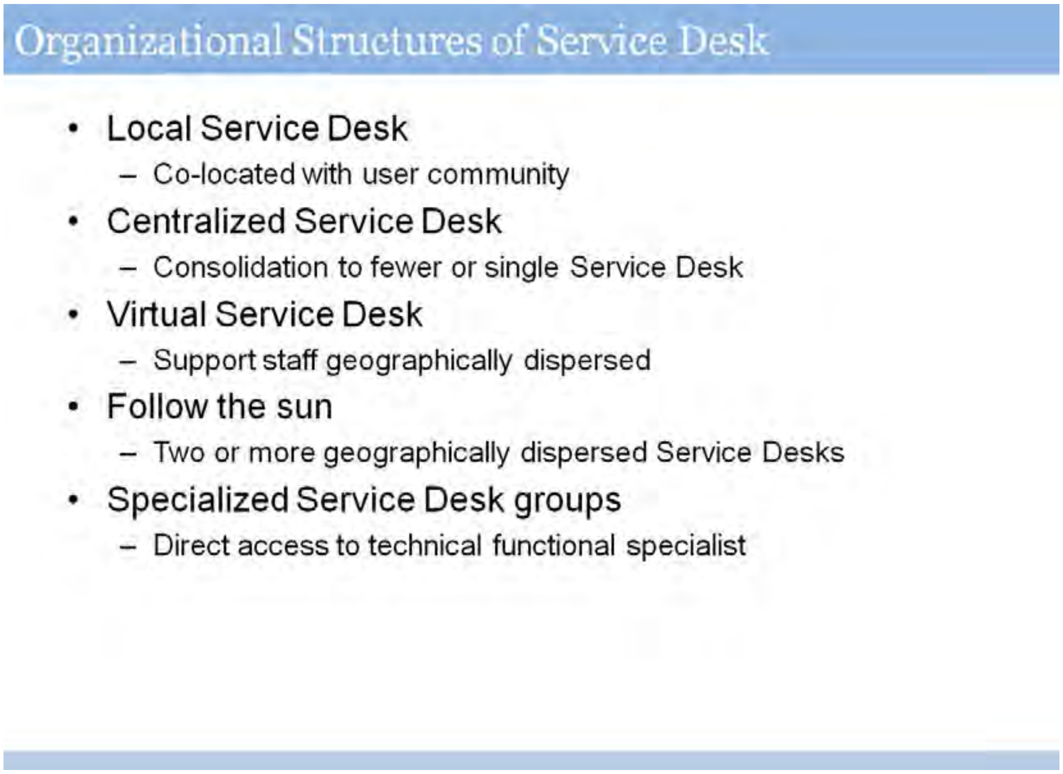
Purpose, Goals & Objectives of the Service Desk

As the single point of contact between IT and its users, the Service Desk function considers its primary objective to log all user-reported Incidents and Requests.

One of the reasons for the blurred line between the Service Desk function and the Incident Management process is that Service Desk staff normally act as first-line support staff for the Incident Management process. In this role, Service Desk staff engage in investigating and diagnosing Incidents and with processing Service Requests. If restoring the impacted service or fulfilling a request exceeds their capabilities, they escalate the Incident or Service Request to second-line support staff members.

Communicating with the customer about the progress of an Incident or Service Request is key to maintaining customer satisfaction, which the Service Desk frequently surveys by either manual or automated means. In addition, in conjunction with the Change Management process, the Service Desk communicates the status and impact of scheduled changes to existing services.

> Typically the Service Desk function also manages the entire Incident Management process, thus the restoration of an IT Service. Although it is tempting to "pass the baton" when an incident escalates to other functional areas in search of higher-level technical skills, such an approach creates a situation where incidents can fall through the cracks.



Organizational Structures of Service Desk

- Local Service Desk
  - Co-located with user community
- Centralized Service Desk
  - Consolidation to fewer or single Service Desk
- Virtual Service Desk
  - Support staff geographically dispersed
- Follow the sun
  - Two or more geographically dispersed Service Desks
- Specialized Service Desk groups
  - Direct access to technical functional specialist

Organizational Structures of Service Desk

The organizational structure of the Service Desk varies, based on the needs of both the business and the IT organization. Some organizations find it necessary to combine two or more of these structures to meet the needs of the business.

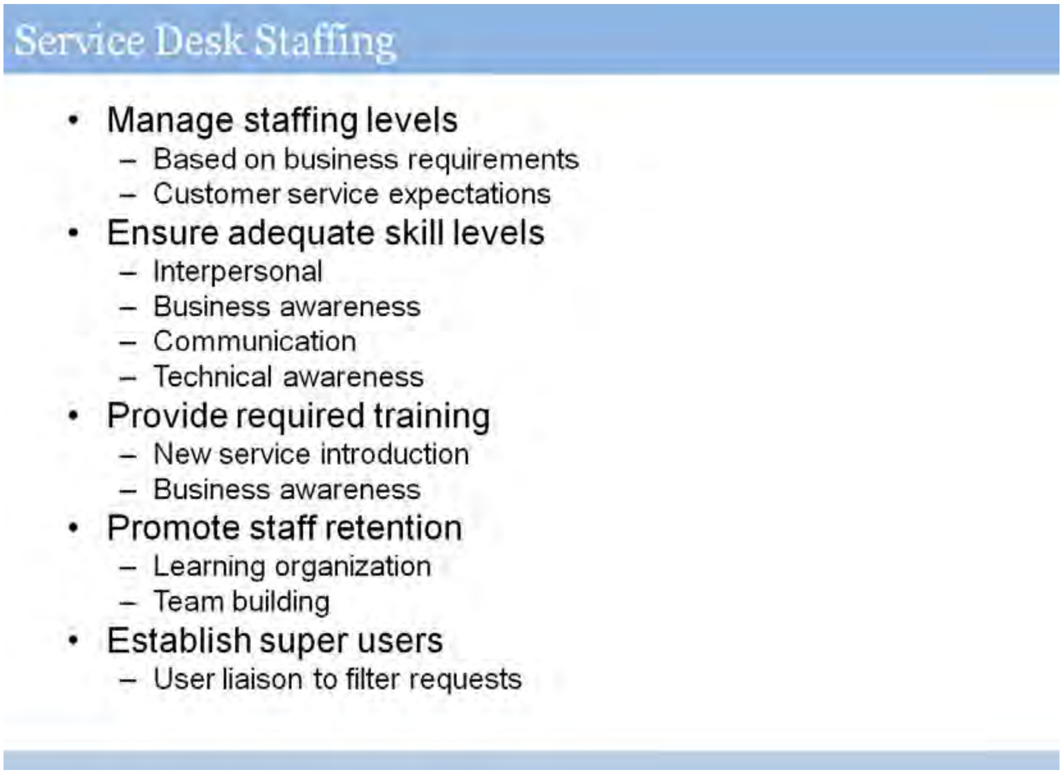
Local - Co-located with the users it serves, a Local Service Desk improves communication but is resource intensive and may lead to significant duplication of resources

Centralized - A Centralized Service Desk may represent a number of individual or local Service Desks, consolidated into a single location. This provides for a better pattern of resource utilization.

Virtual - A Virtual Service Desk utilizes technology to provide the appearance of a centralized Service Desk. This structure may allow the required resources to be located anywhere and enables the inclusion of specialized groups that normally could not be part of a centralized structure

Follow-the-Sun - As the name implies, a Follow the Sun approach uses multiple Service Desk locations tied together via technology and situated in locations around the globe. This enables an IT organization with a worldwide presence to offer 24-hour Service Desk availability without the expense of paying an off-shift differential.

Specialized Service Desk Groups - Technology can support the creation of specialist groups within an organization and allow direct routing



Service Desk Staffing

- Manage staffing levels
  - Based on business requirements
  - Customer service expectations
- Ensure adequate skill levels
  - Interpersonal
  - Business awareness
  - Communication
  - Technical awareness
- Provide required training
  - New service introduction
  - Business awareness
- Promote staff retention
  - Learning organization
  - Team building
- Establish super users
  - User liaison to filter requests

Service Desk - Staffing

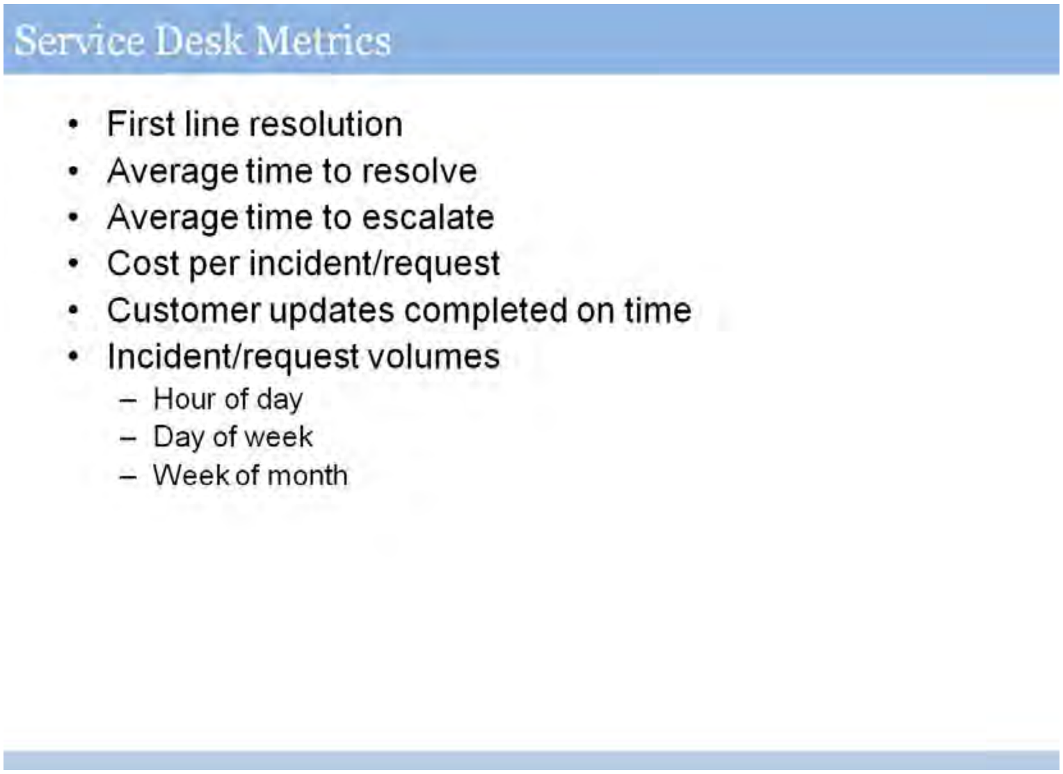
Staffing Level - The business' demand for its resources should establish the base criteria for Service Desk staffing levels and should include variations in that demand based on the natural cycles of the business.

Skill Levels- Selected for their existing skills, Service Desk staff members should further hone their skills by training to improve their interpersonal skills, their awareness of the business they support, their ability to communicate effectively, and the necessary technical skills to support the IT services.

Training - Service Desk staff should receive on-going skills training. In addition, part of the transition of new services to operations is support staff training on the new service. The Service Desk staff is normally a very tightly knit organization that must work well with other Incident and Request Fulfillment staff members. Team-building skills facilitate the establishment of closer working relationships within IT.

Retention - The retention of Service Desk personnel is key to the long-term success of the Service Desk function, Incident Management and the Request Fulfillment processes. Management should clearly establish the appropriate career path planning and salary structure, as well as promotion possibilities, to ensure the retention of high-quality Service Desk staff members

Super Users - Under some circumstances, it may be advantageous to designate individuals within specific business units as “Super Users.” They receive special training and act as a liaison between the Service Desk staff and the business users. This is an effective approach if specialized business knowledge provides critical input in facilitating the restoration of service or filtering requests.

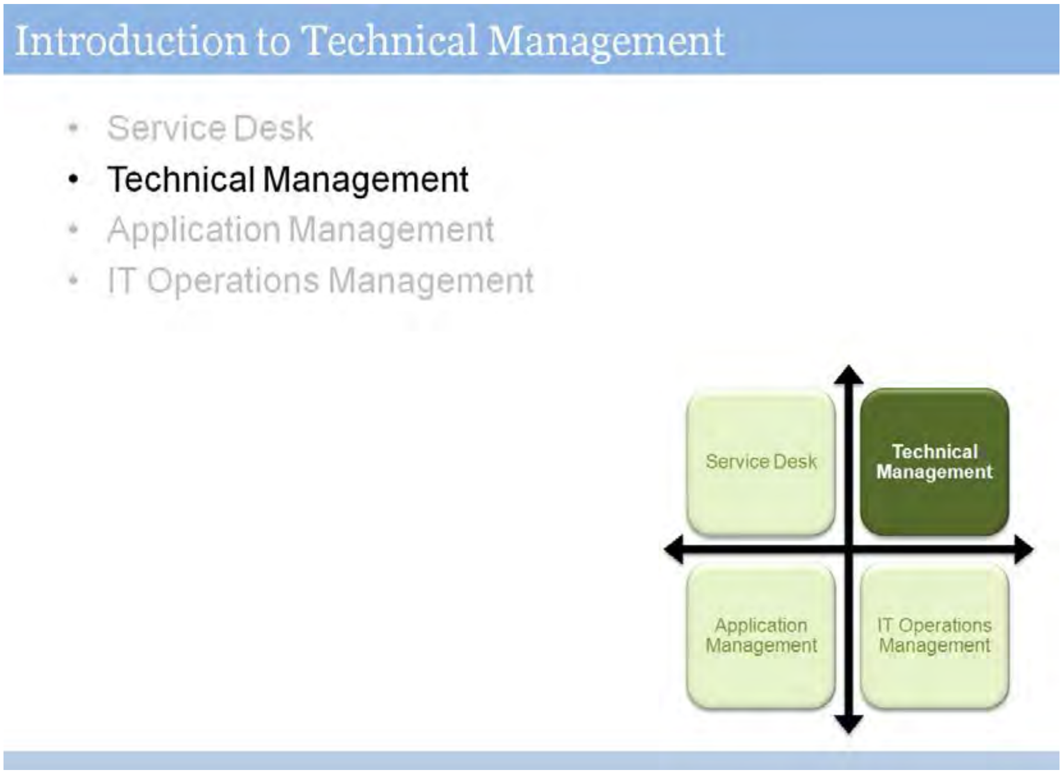


Service Desk Metrics

- First line resolution
- Average time to resolve
- Average time to escalate
- Cost per incident/request
- Customer updates completed on time
- Incident/request volumes
  - Hour of day
  - Day of week
  - Week of month

Service Desk - Metrics

As with all processes and functions, it is important to identify the desired outcomes and the metrics that can help manage the achievement of those outcomes. The list above is representative of some typical Service Desk metrics, but does not present a full list. The outcomes and measures will change over time as the organization, functions and processes mature.



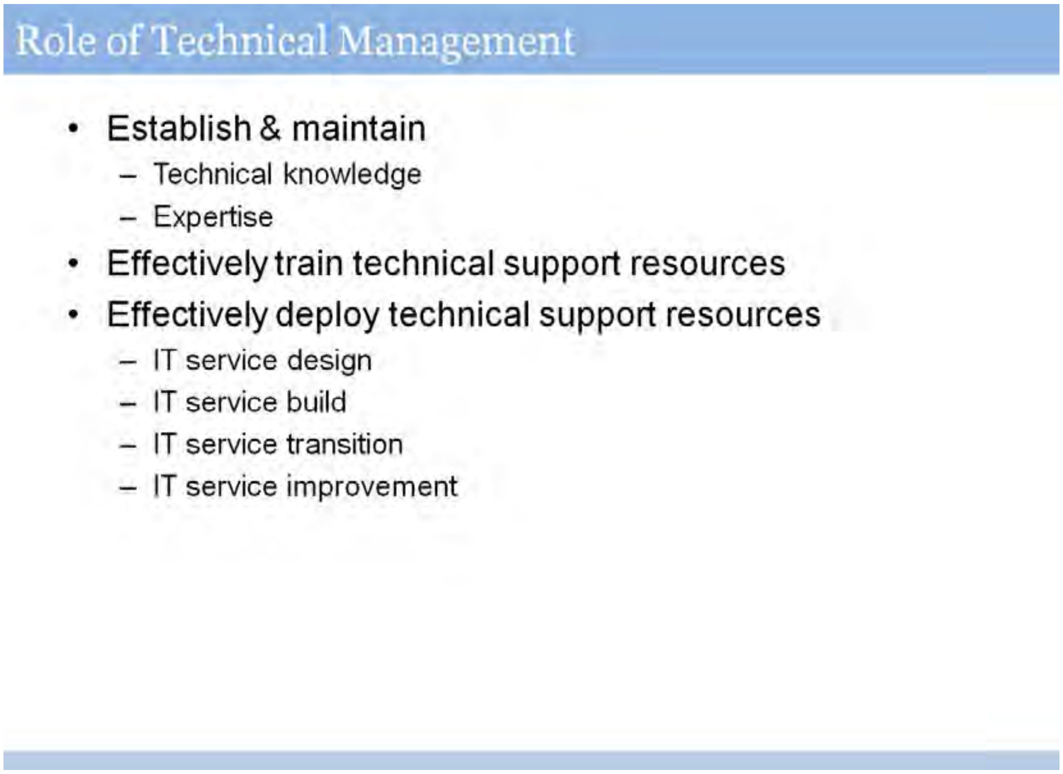
Introduction to Technical Management

- Service Desk
- Technical Management
- Application Management
- IT Operations Management

Service Desk
Technical Management
Application Management
IT Operations Management

Introduction to Technical Management

ITIL defines a function as, “a team or group of people and the tools they use to carry out one or more processes or activities.” Within the Service Operation Lifecycle domain, the Technical Management function provides the technical expertise and resources for the overall management of the IT infrastructure, thus its IT Services. It works in conjunction with the other Service Operation functions; Service Desk, IT Operations and Application Management.



Role of Technical Management

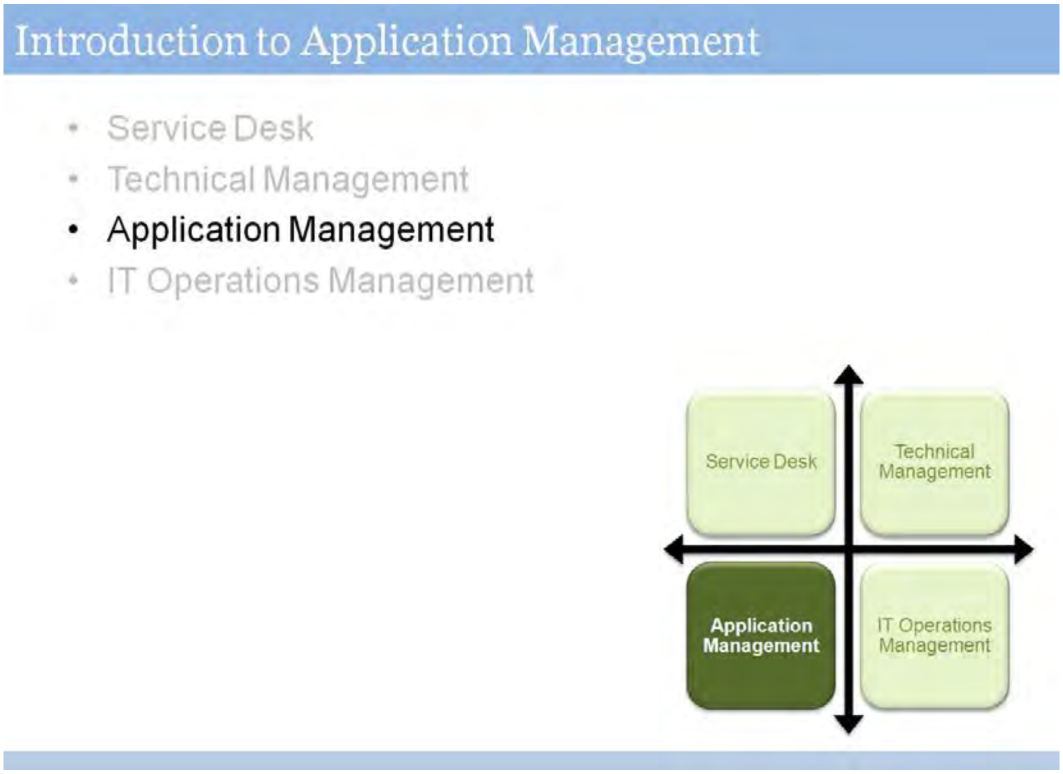
- Establish & maintain
  - Technical knowledge
  - Expertise
- Effectively train technical support resources
- Effectively deploy technical support resources
  - IT service design
  - IT service build
  - IT service transition
  - IT service improvement

Role of Technical Management

Similar to the Application Management Function, Technical Management plays two roles within the Service Operation domain.

Its first role is to establish and maintain the technical knowledge and expertise within the function to support the design, creation, transition, operation and improvement of IT Services. This requires the IT organization to carefully balance the cost of acquiring and maintaining the necessary expertise to its benefit in the support of IT Services. IT organizations may employ different strategies that range from the exclusive use of internal IT staff to the exclusive use of external staff (contract employees) or any combination of the two extremes.

Its second role is to provide the actual resources; the "hands and feet" necessary to support the IT Service Lifecycle processes as well as perform the technical support tasks and activities of the function. This requires that skill levels are established and maintained at the required levels to support the process and IT Services. In addition, these resources play an integral role in the actual design of IT Services, their creation (the build) and the subsequent transition of IT Services into operation and ongoing efforts to improve their value to the business.

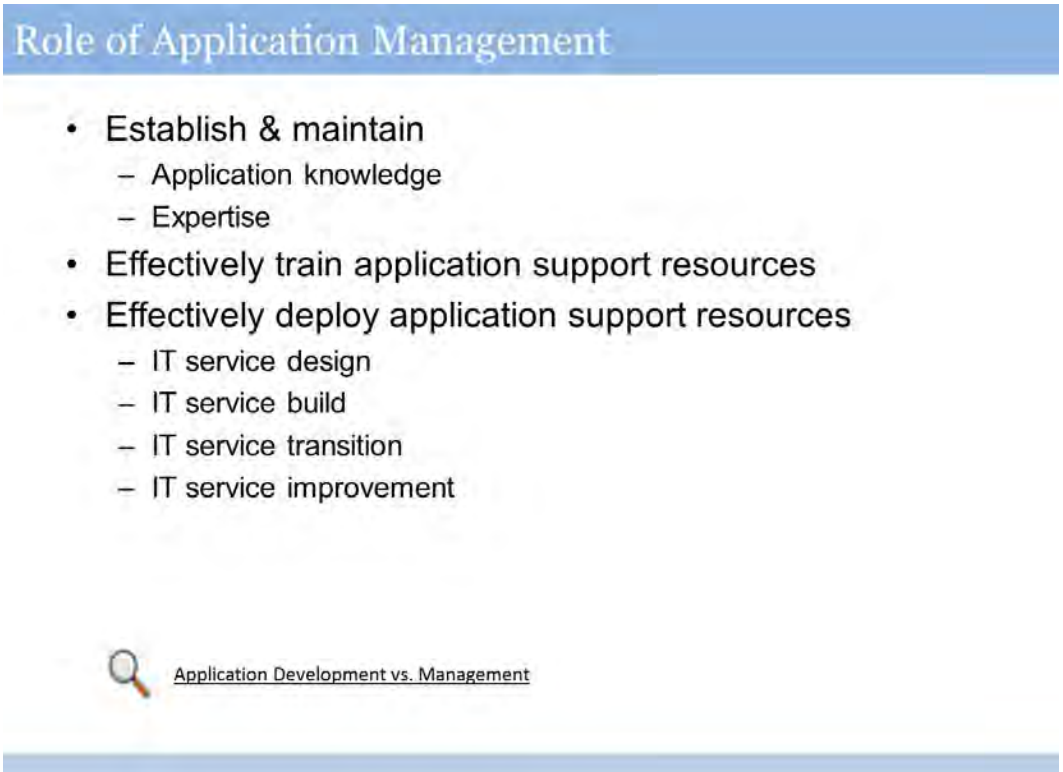


Introduction to Application Management

- Service Desk
- Technical Management
- Application Management
- IT Operations Management

Introduction to Application Management

Application Management manages the enterprise's applications throughout their lifecycle. It is similar to the Technical Management Function because it provides expertise and resources to the enterprise for planning, designing, developing, transitioning, operating and improving the applications used within IT Services to support business processes.



Role of Application Management

- Establish & maintain
  - Application knowledge
  - Expertise
- Effectively train application support resources
- Effectively deploy application support resources
  - IT service design
  - IT service build
  - IT service transition
  - IT service improvement

Application Development vs. Management

Role of Application Management

Similar to the Technical Management Function, Application Management plays two roles within the Service Operation phase.

Its first role is to establish and maintain technical knowledge and expertise within the function to support the design, creation, transition, operation and improvement of applications within IT Services. This requires the IT organization to balance the cost of acquiring and maintaining the necessary expertise against the benefit received in supporting the applications.

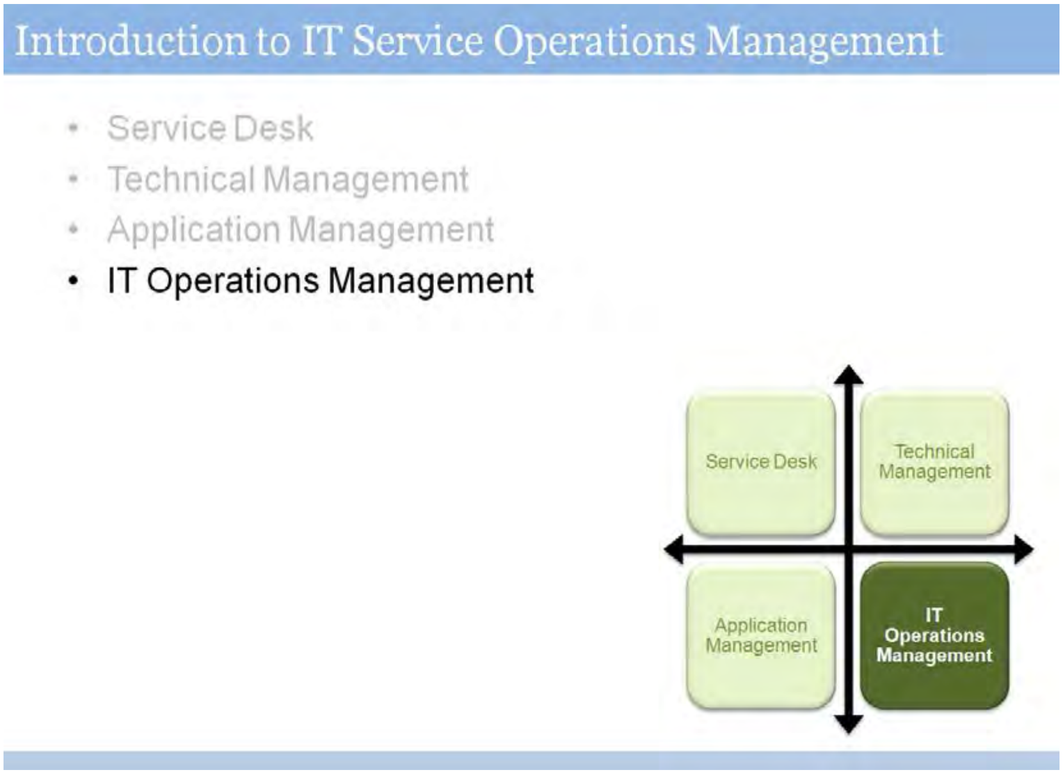
IT organizations may employ different strategies that range from the exclusive use of internal IT staff to the exclusive use of external staff (contract employees) or any combination of the two extremes. This also includes enterprise application suites (ERP, MRP and HR) that support the business' major business functions.

Application Management's second role is to provide the actual resources necessary to support the IT Service Lifecycle processes, as well as perform the function's support tasks and activities. This requires that Application Management establish and maintain skill sets at the required levels to support the process and IT Services.

These resources play an integral role in designing the applications within IT Services, creating them (the build), subsequently transitioning the applications into operation, and continuing efforts to improve its value to the business.

There are differences between Application Development and the Application Management Function: application development deals with a specific instance of a development effort, while Application Management deals with the continual management of all applications regardless of source (See table below).

	Application Development	**Application Management**
Activities	Limited to specific development instance	Continual management of applications throughout their entire lifecycle
Scope	Normally for internally developed applications	Performed for all applications; internally developed or purchased
Focus	Utility focus; fit for purpose	Utility & warranty focus
Management	Managed via Project Management methods (beginning, middle & end)	Managed via process (on-going)
Measurement	Creativity & completion	Consistency & avoidance of incidents/problem, etc.
Cost	Resources are known and quantifiable	Difficult to measure due to dispersed and shared resources
Lifecycle	Software Development Lifecycle	IT Service Management Lifecycle; Service Operation & Continual Service Improvement



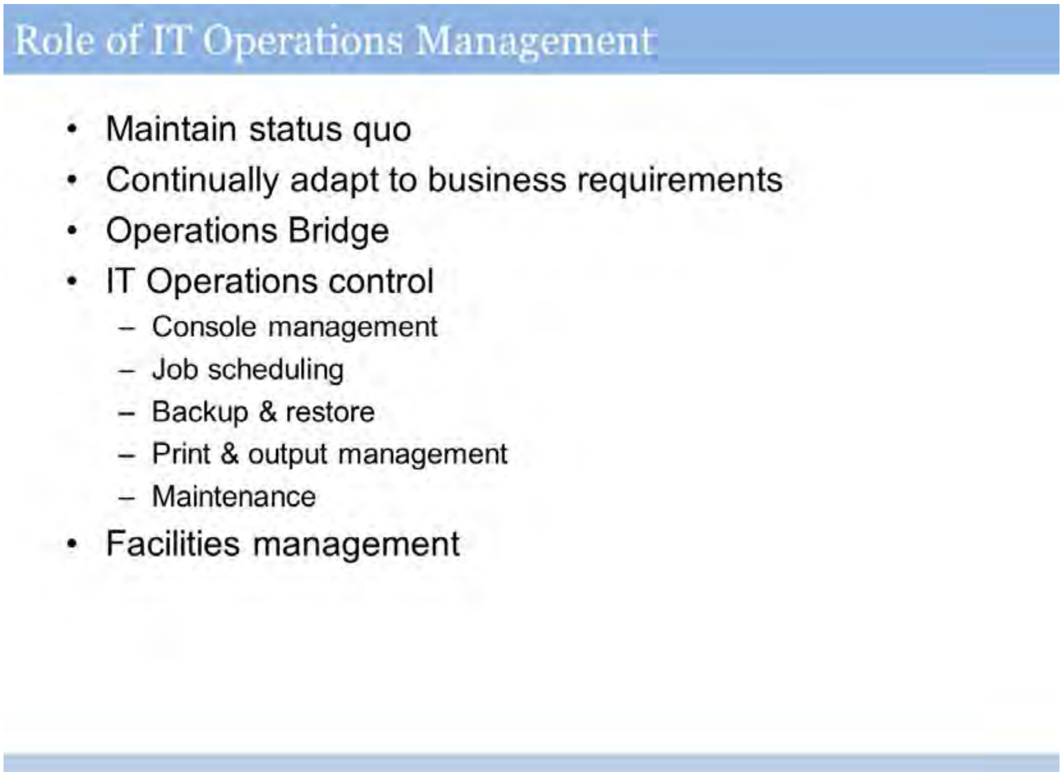
Introduction to IT Service Operations Management

- Service Desk
- Technical Management
- Application Management
- IT Operations Management

Service Desk
Technical Management
Application Management
IT Operations Management

Introduction to IT Service Operations Management

ITIL defines a function as “a team or group of people and the tools they use to carry out one or more processes or activities.” Within the Service Operation Lifecycle domain, the IT Operations Management Function performs the day-to-day activities involved in ongoing management and maintenance of the IT infrastructure. Its purpose is the delivery of IT Services at agreed levels to meet stated business objectives..



Role of IT Operations Management

- Maintain status quo
- Continually adapt to business requirements
- Operations Bridge
- IT Operations control
  - Console management
  - Job scheduling
  - Backup & restore
  - Print & output management
  - Maintenance
- Facilities management

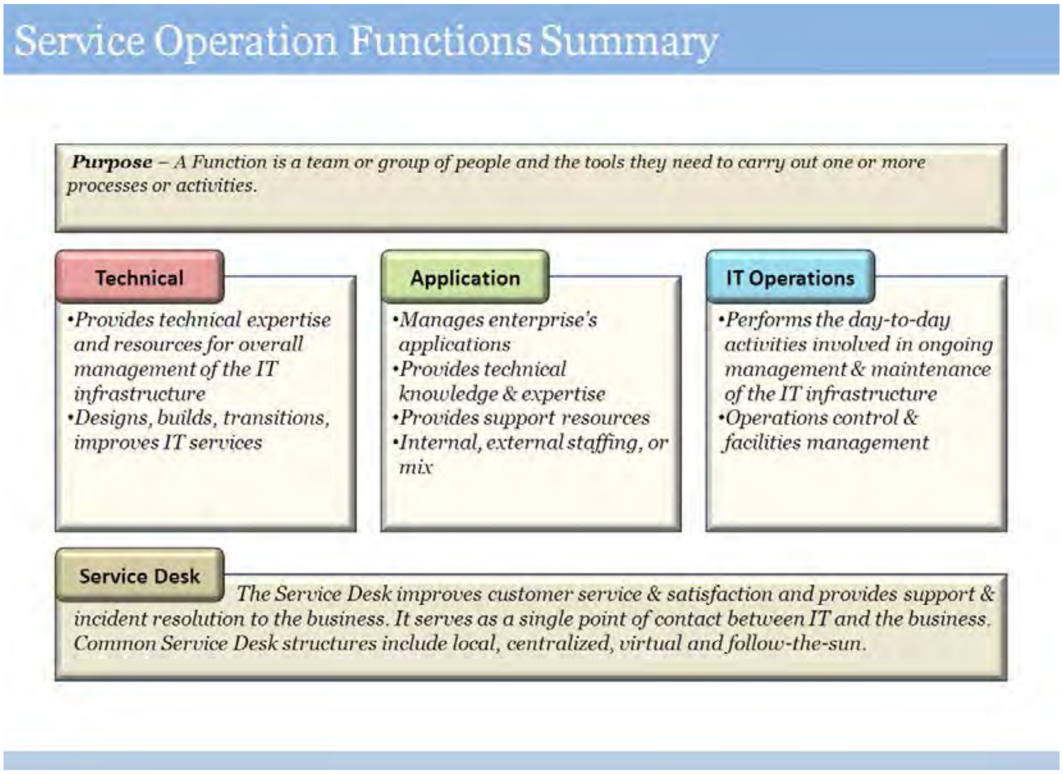
Role of Operations Management

Operations Management plays a dual role similar to other Service Operation functions.

First, it maintains the status quo. It executes clearly defined procedures within clearly defined activities within clearly defined processes. IT Operations drives the stability of the delivery of an IT Service, which helps ensure the consistency of the IT Service.

Its second role is to add value in support of the enterprise value network. It accomplishes this through the day-to-day delivery of stable IT Services, while maintaining constant watch on the business' IT Service support requirements. While compelled to maintain stability in the delivery of services, it must remain flexible and responsive to changing business needs.

IT Operations control may be consolidated in a single location where IT Services and Infrastructure can be monitored and managed. This is often referred to as the Operations Bridge or Network Operation Center (NOC). Here, the actual activities of IT Operations run the gamut from console management to managing the printed output of applications. They also extend to managing the physical environment in which the IT infrastructure operates, such as the computer room, recovery sites, heating ventilation and air conditioning (HVAC), and electrical power distribution and backup.



Service Operation Functions Summary

Purpose *– A Function is a team or group of people and the tools they need to carry out one or more processes or activities.*

Technical

- *Provides technical expertise and resources for overall management of the IT infrastructure*
- *Designs, builds, transitions, improves IT services*

Application

- *Manages enterprise's applications*
- *Provides technical knowledge & expertise*
- *Provides support resources*
- *Internal, external staffing, or mix*

IT Operations

- *Performs the day-to-day activities involved in ongoing management & maintenance of the IT infrastructure*
- *Operations control & facilities management*

Service Desk

The Service Desk improves customer service & satisfaction and provides support & incident resolution to the business. It serves as a single point of contact between IT and the business. Common Service Desk structures include local, centralized, virtual and follow-the-sun.

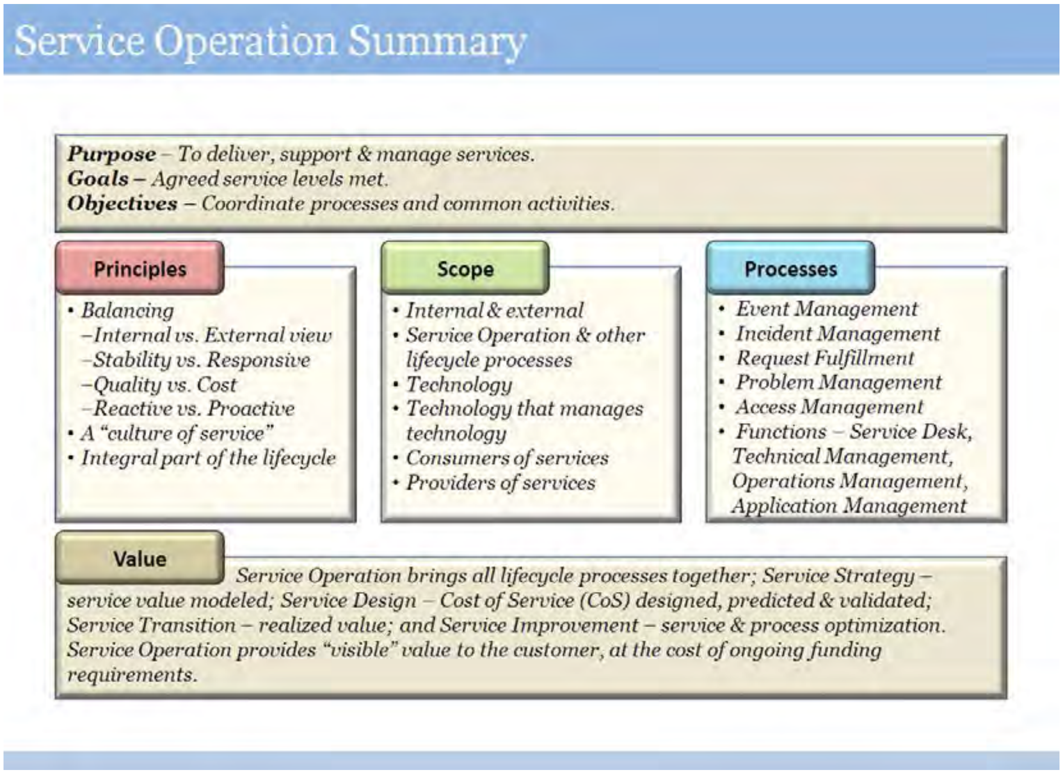
Service Operation Functions Summary

The Service Operation phase of the service lifecycle encompasses four functions. The Service Desk serves as the single point of contact between IT and the user, and, as such, presents the "face" of IT to the user. As a result, it improves customer service and customer satisfaction with IT. Common Service Desk structures are local, centralized, virtual, and "follow-the-sun."

Application Management performs the day-to-day activities of managing installed applications, and Technical Management provides the technical skills and expertise for overall management of the IT infrastructure. It also participates in design, build and implementation activities. Finally, IT Operations Management performs the day-to-day "touch" activities involved in ongoing management and maintenance of the IT infrastructure. It also provides operations control and facilities management.

Lesson 12

Service Operation Summary



Service Operation Summary

Purpose – *To deliver, support & manage services.*
Goals – *Agreed service levels met.*
Objectives – *Coordinate processes and common activities.*

Principles

- *Balancing*
  - *Internal vs. External view*
  - *Stability vs. Responsive*
  - *Quality vs. Cost*
  - *Reactive vs. Proactive*
- *A "culture of service"*
- *Integral part of the lifecycle*

Scope

- *Internal & external*
- *Service Operation & other lifecycle processes*
- *Technology*
- *Technology that manages technology*
- *Consumers of services*
- *Providers of services*

Processes

- *Event Management*
- *Incident Management*
- *Request Fulfillment*
- *Problem Management*
- *Access Management*
- *Functions – Service Desk, Technical Management, Operations Management, Application Management*

Value

Service Operation brings all lifecycle processes together; Service Strategy – service value modeled; Service Design – Cost of Service (CoS) designed, predicted & validated; Service Transition – realized value; and Service Improvement – service & process optimization. Service Operation provides "visible" value to the customer, at the cost of ongoing funding requirements.

Service Operation Summary

Service Operation is the heartbeat of the IT service provider. It is where all the improvements, strategy, design and transitions culminate to provide IT services to the business customer.

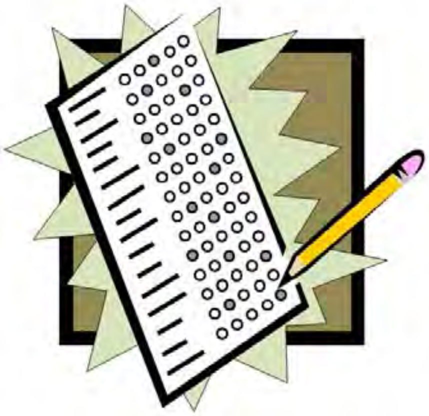
Effective and efficient Service Operation is always a balancing act. It balances what the IT service provider needs to know to do its job against what the customer sees and understands about IT services, and it balances between the stability of continually refining an existing IT service and responsiveness to the constantly changing needs of the business. It also balances the quality of IT services against the cost to provide increasing levels of quality, and the allocation of staff to reactive support versus proactive development.

Its scope extends over the entire organization, as well as external service providers. It actively participates in other phases of the IT Service Lifecycle to ensure the integration of new services into the operational environment.

Service Operation encompasses five processes (Event Management, Incident Management, Frequent fulfillment, Problem Management, and Access Management) and four functions (Service Desk, Technical Management, Operations Management and Application Management).

Finally, Service Operation provides value to the business by successfully providing operational services.

Checkpoint



Checkpoint Instructions

The Checkpoint is an end-of-chapter quiz. It checks your understanding and knowledge of the fundamental concepts and principles of the Continual Service Improvement phase of the IT Service Management Lifecycle. It uses Bloom's Level 1 & 2 type questions; i.e., recall, recite, name, and understand the meaning of ITIL terminology and basic practice fundamentals. This correlates to the level of the ITIL Foundation certification examination.

This quiz is a preparation exercise for the ITIL Foundation certification exam. Sample papers for the certification exam are available at the end of the course.

The Checkpoint quiz employs different question types, such as multiple choice, multiple answer (more than one correct answer), partial credit (accumulate points for the correct parts of an answer), fill-in-the-blank, sequence (put things in the correct order) and matching. Answers and their rationale follow the quiz. Each question is worth 10 points for a total of 100 points for the quiz. The passing score is 75.

Good luck!

ITIL v3 Glossary

A

Acceptance
Formal agreement that an IT Service, process, plan, or other deliverable is complete, accurate, reliable and meets its specified requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a project or process.

Access Management
The Process responsible for allowing users to make use of IT Services, data, or other assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized users are able to access or modify the assets. Access Management is sometimes referred to as Rights Management or Identity Management.

Account Manager
A role that is very similar to Business Relationship Manager, but includes more commercial aspects. Most commonly used when dealing with external customers.

Accounting
The Process responsible for identifying actual Costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.

Accredited
Officially authorized to carry out a role. For example, an Accredited body may be authorized to provide training or to conduct audits.

Active Monitoring
Monitoring of a Configuration Item or an IT Service that uses automated regular checks to discover the current status.

Activity
A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans, and are documented in procedures.

Agreement
A document that describes a formal understanding between two or more parties. An dgreement is not legally binding unless it forms part of a contract.

Alert
A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.

Application
Software that provides functions that are required by an IT Services. Each Application may be part of more than on IT Service. An Application runs on one or more Servers or Clients. See also Application Management, Application Portfolio.

Application Management
The Function responsible for managing Applications throughout their lifecycle.

Application Portfolio
A database or structured document used to manage Applications throughout their lifecycle. The Application Portfolio contains key attributes of all applications. The Application Portfolio is sometimes implemented as part of the Service Portfolio, or as part of the Configuration Management System.

Application Sizing
The activity responsible for understanding the resource requirements needed to support a new application, or a major change to an existing application. Application Sizing helps to ensure that the IT Service can meet it agreed Service Level Targets for capacity and performance.

Architecture
The structure of a system or IT Service, including the relationships of components to each other and to he environment they are in. Architecture also includes the standards, and guidelines that guide the design and evolution of the system.

Assessment
Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effusiveness targets are being met.

Asset
Any Resource or Capability. Assets of a Service Provider including 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, and Financial Capital.

Asset Management
Asset Management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.

Attribute
A piece of information about a Configuration Item. Examples are; name, location, Version number and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB).

Audit
Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. An Audit may be carried out by internal or external groups.

Authority Matrix
See RACI

Automatic Call Distribution (ACD)
Use of the information Technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.

Availability
Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measures of the Business output of the IT Service.

Availability Management
The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, roles, etc. are appropriate for the agreed Service Level Targets for availability.

Availability Management Information System (AMIS)
A set of tools, data and information that is used to support Availability Management. See also Service Knowledge Management System.

Availability Plan
A plan to ensure that existing and future Availability Requirements for IT Services can be provided cost effectively.

B

Back-out
See Remediation

Backup
Copying data to protect against loss of Integrity or Availability of the original.

Balanced Scorecard
A management tool developed by Drs. Robert Kaplan (Harvard Business School) and David Norton, A Balanced Scorecard enables a Strategy to be broken down into Key Performance Indicators. Performance against the KPIs is used to demonstrate how well the Strategy is being achieved. A Balanced Scorecard has four major areas, each of which has a small number of KPIs. The same four areas are considered at different levels of detail throughout the Organization.

Baseline
A Benchmark used as a reference point. For example: An ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan. A Performance Baseline can be used to measure change in Performance over the lifetime of an IT Service. A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails.

Benchmark
The recorded state of something at a specific point in time. A Benchmark can be created for a configuration, a process, or any other set of data. For example, a benchmark can be used in Continual Service Improvement, to establish the current state for managing improvements or Capacity Management, to document performance characteristics during normal operations.

Benchmarking
Comparing a Benchmark with a Baseline or with Best Practice. The term Benchmarking is also used to mean creating a series of Benchmarks over time, and comparing the results to measure progress or improvement.

Best Management Practice (BMP)
The Best Management Practice portfolio is owned by the Cabinet Office, part of HM Govermnent. The BMP portfolio includes guidance on IT Service Management and Project, Program, Risk Portfolio and Value Management.

Best Practice
Proven Activities or Processes that have been successfully used by multiple Organizations. ITIL is an example of Best Practice.

Billing
Part of the charging proces. Billing is the activity responsible for producing an invoice or a bill and recovering the money from customers. See also Pricing.

Brainstorming
A technique that helps a team to generate ideas. Ideas are not reviewed during the Brainstorming session, but at a later stage. Brainstorming is often used by Problem Management to identify possible causes.

British Standards Institution (BSI)
The UK national standards body, responsible for creating and maintaining British Standards.

Budget
A list of all the money an organization or business Unit plans to receive, and plans to pay out, over a specified period of time.

Budgeting
The Activity of predicting and controlling the spending of money. Consists of a periodic negotiation cycle to set future budgets (usually annual) and the day-to-day monitoring and adjusting of current budgets.

Build
The Activity of assembling a number of Configuration Items to create part of an IT Service. The term Build is also used to refer to a release that is authorized for distribution. For example Server Build or laptop Build.

Business
An overall corporate entity or organization formed of a number of Business Units. In the context of ITSM, the term Business includes public sector and not-for-profit organizations, as well as companies. An IT Service Provider provides IT Services to a customer within a Business. The IT Service Provider may be part of the same Business as its customer (Internal Service Provider), or part of another Business (External Service Provider).

Business Capacity Management
In the context of ITSM, Business Capacity Management is the sub-process of Capacity Management responsible for understandng future business requirements for use in the Capacity Plan.

Business Case
Justification for a significant item of expenditure. Includes information about costs, benefits, options, issues, Risks, and possible problems.

Business Continuity Management
The business process responsible for managing risks that could seriously affect the business.

Business Customer
A recipient of a product or a service from the business. For example, if the business is a car manufacturer then the business customer is someone who buys a car.

Business Impact Analysis (BIA)
BIA is the activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other business processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.

Business Objective
The Objective of a business process, or of the business as a whole. Business Objectives support the business vision, provide guidance for the IT Strategy, and are often supported by IT Services.

Business Operations
The day to day execution, monitoring and management of business processes.

Business Perspective
An understanding of the Service Provider and IT Services from the point of view of the business, and an understanding of tthe business from the point of view of the Service Provider.

Business Process
A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or service to a business customer.

Business Relationship Management
The process or function responsible for maintaining a relationship with the business. Business Relationship Management usually includes: managing personal relationships with usiness managers, providing input to Service Portfolio Management, ensuring that the IT Service Provider is satisfying the business needs of the customers.

Business Relationship Manager
A role responsible for maintaining the relationship with one or more customers. This role is often combined with the Service Level Manager role.

Business Service
An IT Service that directly supports a business process, as opposed to an infrastructure service, which is used internally by the IT Service Provider and is not usually visible to the business.

Business Service Management (BSM)
An approach to the management of IT Services that considers the business processes supported and the Business value provided. The term also means the management of Business Services delivered to business customers.

Business Unit
A segment of the business that has its own plans, Metrics, income and costs. Each Busi-

ness Unit owns assets and uses these to create value for customers.

C

Call
A telephone call to the Service Desk from a user. A call could result in an incident or a Service Request being logged.

Call Center
An Organization or Business Unit that handles large numbers of incoming and outgoing telephone calls.

Call Type
A Category that is used to distinguish incoming requests to a Service Desk. Common call types are Incident, Service Request and Complaint.

Capability
The ability of an organization, person, process, application, IT Service or other Configuration Item to carry out an activity. Capabilities are intangible assets of an organization. See also resource.

Capability Maturity Model Integration (CMMI)
A process improvement appoach developed by the Software Engineering Institue (SEI) of Carnegie Mellon University. CMMI provides organizations with the essential elements of effetive processes.It can be used to guide process improvement across a project, a division or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorties, provide guidance for quality processes and current process.

Capacity
The maximum throughput that a Configuration Item or IT Service can deliver while meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.

Capacity Management
The process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service and plans for short, medium and long term business requirements.

Capacity Management Information System
A set of tools, data and information that is used to support Capacity Management See also Service Knowledge Management System.

Capacity Plan
A Capacity Plan is used to manage the resources required to deliver IT Services. The plan contains scenarios for different predictions of business demand, and costed options to deliver the agreed Service Level Targets.

Capacity Planning
The Activity within Capacity Management responsible for creating a Capacity Plan.

Capital Cost
The cost of purchasing something that will become a financial asset. The value of the asset depreciates over multiple accounting periods.

Capital Expenditure (CAPEX)
The cost of purchasing something that will become a financial asset, for example, computer equipment and buildings. The value of the asset is depreciated over multiple accounting periods.

Category
A named group of things that have something in common. Categories are used to group similar things together. For example, Cost Types are used to group similar types of Cost, Incident Categories are used to group similar types of Incidents, CI Types are used to group similar types of configuration Items.

Certificate
Issuing a certificate to confirm Compliance to a standard. Certification includes a formal audit by an independent and accredited body. The term Certification is also used to mean

awarding a certificate to verify that a person has achieved a qualification.

Certification
Issuing a certificate to confirm compliance to a standard. Cetrification includes a formal audit by an independent and accredited body. The term is also use dto men awading a certificate to provide evidence that a person ahas acheived a qualification.

Change
The addition, modification or removal of anything that could have an effect on IT Services. The scope should include all IT Services, Configuration Items, processes, documentation, etc.

Change Advisory Board (CAB)
A group of people that advises the Change Manager in the assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the business and third parties such as suppliers.

Change Case
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.

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.

Change Management
The process responsibile for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT Services.

Change Model
A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). See also Standard Change, Change Advisory Board.

Change Proposal
A document that includes a high level description of a potential service introduction or significant change along with a corresponding business case and an expected implementation schedule. Change proposals are normally created by the Service Portfolio Management process and are passed to Change Management for authorization. Change Management will review the potential impact on other services, on shared,r-esources, and on the overall change schedule. Once the change proposal has been authorized, Service Portfolio Management will charter the service.

Change Record
A Record containing the details of a Change. Each Change Record documents the lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.

Change Schedule
A document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.

Charging
Requiring payment for IT Services. Charging for IT Services is optional and many Organizations choose to treat their IT Service Provider as a Cost Center.

Charging Policy
A policy specifiying the objective of the charging process and the way in which charges will be calculated.

Charging Process
The process responsible for deciding how much customer should pay (pricing) and recovering money from them (billing). This process is not described in detail within the core ITIL publications.

Charter
A document that contains details of a new service, a signficant change or other significant project. Charters are typically authorized by Service Portfolio Managmeent or by a Project Management Office. The term charter is also used to describe the act of authorizing the work required to complete the service change or project.

Chronological Analysis
A technique used to help identify possible causes of Problems. All available data about the problem is collected and sorted by date and time to provide a detailed time line. This can make it possible to identify which events may have been triggered by others.

Classification
The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes etc. are usually classified.

Client
A generic term that means a Customer, the Business or a Business Customer. For example, Client Manager may be used as a synonym for Accounting Manager.

Closed
The final status in the Lifestyle of an Incident, Problem, Change etc. When the status is closed no further action is taken.

Closure
The act of changing the Status of an Incident, Problem, Change etc. to Closed.

CoBIT
Control Objectives for information and related Technology (CoBIT) provides guidance and Best Practice for the management of IT Processes. CoBIT is published by the IT Governance Institute. See www.isaca.org for more information.

Code of Practice
A guideline published by a public body or a standards organization, such as ISO or BSI. Many standards consist of a code of practice and a specification. The code of practice describes recommended best practice.

Commercial Off-The-Shelf (COTS)
Application software or Middleware that can be purchased from a Third Party.

Compliance
Ensuring that a Standard or a set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.

Component
A general term that is used to mean one part of something more complex. For example, a computer System may be a Component of an IT Service, an Application may be a Component of a Release Unit. Components that need to be managed should be Configuration Items.

Component Capacity Management
The Process responsible for understanding the Capacity, Utilization and Performance of Configuration Items. Data is collected, recorded and analyzed for use in the Capacity Plan. See also Service Capacity Management.

Component CI
A Configuration Item that is part of an assembly. For example, a CPU or memory CI may be part of a server CI.

Component Failure Impact Analysis (CFIA)
A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure.)

Computer Telephony Integration (CTI)
Computer telephony Integration (CTI) is a general term covering any kind of integration between computers and telephone Systems. It is most commonly used to refer to systems where an application displays detailed screens relating to incoming or outgoing telephone

calls. See also Automatic Call distribution, Interactive Voice Responses.

Concurrency
A measure of the number of Users engaged in the same Operation at the same time.

Confidentiality
A security principle that requires that data should only be accessed by authorized people.

Configuration
A generic term used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.

Configuration Baseline
The baseline of a configuration that has been formally agreed and is managed through the Change Management process. A Configuration Baseline is used as a basis for future builds, releases and changes.

Configuration Control
The activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.

Configuration Item (CI)
Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management
The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifestyle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

Configuration Management Database (CMDB)
A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.

Configuration Management System (CMS)
A set of tools and databases that are used to manage an IT Service Provider’s Configuration Data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and it may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See also Configuration Management Database, Service Knowledge Management System.

Continual Service Improvement (CSI)
A stage in the Lifestyle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services, and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See also Plan-Do-Check-Act.

Contract
A legally binding Agreement between two or more parties.

Control
A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example: Controls include policies, procedures, roles, RAID, door locks etc. A Control is sometimes called a countermeasure or safeguard. Control also

means to manage the utilization or behavior of a Configuration Item, System or IT Service.

Control Objective
An approach to the management of IT Services, Processes, Functions, Assets, etc. There can be several different Control Perspectives on the same IT Service, Process, etc., allowing different individuals or teams to focus on what is important and relevant to their specific Role. Example Control Perspectives include Reactive and Proactive management with IT Operations, or a Lifecycle view for an Application Project team.

Control Objectives for Information and related Technology (CoBIT)
See CoBIT.

Control Perspective
An approach to the managemetn of IT Services, processes, functions, assets tec. There can be several different Control Perspectives on the same IT Services, process etc., allowing different individuals or teams to focus on what is important and relevant to their specific role.

Core Service
A service that delivers the basic outcomes desired by one or more customers. A Core Service provides a specific level of utility and warranty. Customers may be offered a choice of utility and warranty through one or more service options.

Cost
The amount of money spent on a specific Activity, IT Service or Business Unit. Costs consist of real cost (money), notional cost such as people's time, and Depreciation.

Cost Benefit Analysis
An Activity that analyses and compares the Costs and the benefits involved in one or more alternative courses of action. See also Business Case.

Cost Center
A business unit or project to which costs are assigned. A Cost Center does not charge for services provided. An IT Service Provider can be run as a Cost Center or a Profit Center.

Cost Effectiveness
A measure of the balance between the Effectiveness and Cost of Service, Process or activity. A Cost Effective Process is one that achieves the Objectives at minimum Cost. See also KPI, Value for Money.

Cost Element
The middle level of category to which costs are assigned in budgeting and accounting. The highest-level category is cost type.

Cost Management
A general term that is used to refer to budgeting and accounting, and is sometimes used as a synonym for Financial Management

Cost Model
A framework used in budgeting and accounting in which all know costs can be recorded, categorized and allocated to specific customers, business units or projects.

Cost Unit
The lowest level of category to which costs are assigned, Cost Units are usually things that can be easily counted or things easily measured. Cost Units are included within cost elements.

Countermeasure
Can be used to refer to any type of Control. The term Countermeasure is most often used when referring to measures that increase Resilience, Fault Tolerance or Reliability of an IT Service.

Course Corrections
Changes made to a plan or activity that has already started to ensure that it will meet its objectives. Course corrections are made as a result of monitoring progress.

Crisis Management
The process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for strategic issues such as managing media relations and shareholder confidence, and decides when to invoke Business Continuity Plans.

Critical success Factor (CSF)
Something that must happen if a Process, Project, Plan or IT Service is to succeed. KPIs

are used to measure the achievement of each CSF. For example a CSF of 'protect IT Services when making Changes' could be measured by KPIs such as 'percentage reduction of unsuccessful Changes', 'percentage reduction in Changes causing Incidents', etc.

CSI Register
A database or structured document used to record and manage improvement opportunities throughout their lifecycle.

Culture
A set of values that is shared by a group of people including expectations about how people should behave, their ideas, beliefs and practices. See also Vision.

Customer
Someone who buys goods or services. The Customer of an IT Service Provider is the person or group that defines and agrees the Service Level Targets. The term Customer is also sometimes informally used to mean Users, for example 'this is a Customer focused Organization.

Customer Agreement Portfolio
A database or structured document used to manage service contracts or agreements between an IT Service Provider and its customers. Each IT Service Delivered to a customer should have a contract or other agreement that is listed in the Customer Agreement Portfolio.

Customer Asset
Any resource or capability of a customer.

Customer-facing Service
An IT Service that is visible to the customer. These are normally services that support he customer’s business process and facilitate one or more outcomes desired by the customer. All live Customer-facing Services, including those available for deployment, are recorded in the Service Catalog along with customer-visible information about deliverables, prices, contact points, ordering and request processes. Other information such as relationships to supporting services and other CIs will also be recorded for internal use by the IT Service Provider.

D

Dashboard
A graphical representation of overall IT Service Performance and Availability. Dashboard images may be updated in real time and can also be included in management reports and web pages. Dashboards can be used to support Service Level Management, Event Management or Incident Diagnosis.

Data-to-Information-to-Knowledge-to-Wisdom (DIKW)
A way of understanding the relationship between data, information, knowledge and wisdom. DIKW show how each of these builds on the others.

Definitive Media Library (DML)
One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.

Deliverable
Something that must be provided to meet a commitment in a Service Level Agreement or a Contract. Deliverable is also used in a more informal way to mean a planned output of any Process.

Demand Management
Activities that understood and influence Customer demand for Services and the provision of Capacity to meet these demands. At a Strategic level Demand Management can involve analysis of Patterns of Business Activity and User Profiles. At a tactical level it can involve use of a Differential Charging to encour-

age Customers to use IT Services at less busy times. See also Capacity Management.

Deming Cycle
See Plan-Do-Check-Act

Dependency
The direct or indirect reliance of one Process or Activity on another.

Deployment
The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc. to the Live Environment. Deployment is part of the Release and Deployment Management Process. See Also Rollout.

Design
An activity or Process that identifies Requirements and then defines a solution that is able to meet these Requirements. See also Service Design.

Design Coordination
The process responsible for coordinating all Service Design activities, processes and resources. Design Coordination ensures the consistent and effective design of new or changed IT Services, Service Management Information Systems, architectures, technology, processes, information and metrics.

Detection
A stage in the incident Lifecycle. Detection results in the Incident becoming known to the Service Provider. Detection can be automatic, or can be the result of a user logging an incident.

Development
The Process responsible for creating or modifying an IT Service or Application. Also used to mean the Role or group that carries out Development work.

Development Environment
The Process responsible for creating or modifying an IT Service or Applications. Development Environments are not typically subjected to the same degree of control as Test Environments or Live Environments. See also Development.

Diagnosis
A stage in the Incident and Problem Lifecycles. The purpose of Diagnosis is to identify a workaround for an Incident or the Root Cause of a Problem.

Diagnostic Script
A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them Classify, Resolve and assign Incidents. Diagnostic Scripts may also be made available to Users to help them diagnose and resolve their own Incidents.

Directory Services
An Application that manages information about IT Infrastructure available on a network, and corresponding User access Rights.

Document
Information in readable form. A Document may be paper or electronic. For example, a Policy statement, Service Level Agreement, Incident Record, diagram of computer room layout. See also Record.

Downtime
The time when a Configuration Item or IT Service is not Available during its Agreed Service Time. The Availability of an IT Service is often calculated from Agreed Service Time and Downtime.

Driver
Something that influences Strategy, Objectives or Requirements. For example, new legislation or the actions of competitors

E

Early Life Support (ELS)
Support provided for a new or Changed IT Service for a period of time after it is Released. During Early Life Support the IT Service Provider may review the KPIs, Service Levels and Monitoring Thresholds, and provide additional Resources for Incident and Problem Management.

Economies of Scale
The reduction in average Cost that is possible from increasing the usage of an IT Service or

Asset.

Economies of Scope
The reduction in cost that is allocated to an IT Service by using an existing asset for an additional purpose. See also Economies of Scale.

Effectiveness
A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives. See also KPI

Efficiency
A measure of whether the right amount of resources has been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. See also KPI.

Emergency Change
A Change that must be introduced as soon as possible. For example, to resolve a Major Incident or implement a security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes. See also Emergency Change Advisory Board (ECAB)

Emergency Change Advisory Board (ECAB)
A subset of the Change Advisory Board that makes decisions about high-impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change

Enabling Service
A Service that is needed in order to deliver a core service. Enabling Services may or may not be visible to the customer, but they are not offered to customers in their own right. See also Enhancing Service

Enhancing Service
A Service that is added to a core service to make it more attractive to the customer. Enhancing Services are not essential to the delivery of a core service but are used to encourage customers to use the core services or to differentiate the Service Provider from its competitors. See also Enabling Service; Excitement Factor

Enterprise Financial Management
The function and process responsible for managing the overall organization's budgeting, accounting and charging requirements. Enterprise Financial Management is sometimes referred to as the "corporate" Financial Department. See also Financial Management for IT Services.

Environment
A subset of the IT Infrastructures that is used for a particular purpose. For Example: Live Environment, Test Environment, Build Environment. It is possible for multiple Environments to share a Configuration Item, for example Test and Live Environment may use different partitions of a single mainframe computer. Also used in the term Physical Environment to mean the accommodation, air conditioning, power system, etc. Environment is also used as a generic term to mean the external conditions that influence or affect something.

Error
A design flow or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that affects a CI or IT Service is also an Error.

Escalation
An Activity that obtains additional Resources when these are needed to meet Service Level Targets or Customer Expectations. Escalation may be needed within any IT Service Management Process, but is most commonly associated with Incident Management, Problem Management and the management of Customer complaints. There are two types of Escalation: Functional Escalation and Hierarchic Escalation.

eSourcing Capability Model for Client Organizations (eSCM-CL)
A framework to help organizations in their analysis and decision-making or service sourcing models and strategies. It was developed by Carnegie Mellon University in the US. See

also eSourcing Capability Model for Service Providers.

eSourcing Capability Model for Service Providers (eSCM-SP)
A framework to help IT Service Providers develop their IT Service Management Capabilities from a Service Sourcing perspective. eSCM-SP was developed by Carnegie Mellon University, US.

Estimation
The use of experience to provide an approximate value for a Metric or Cost. Estimation is also used in Capacity and Availability Management as the cheapest and least accurate Modeling method.

Evaluation
The Process responsible for assessing a new or Changed IT Service to ensure that Risks have been managed and to help determine whether to proceed with the Change.

Event
A change of state that has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions and often lead to Incidents being logged.

Event Management
The process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations.

Exception Report
A Document containing details of one or more KPIs or other important targets that have exceeded defined Thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem.

Excitement Factor
An attribute added to something to make it more attractive or more exciting to the customer. See also Enhancing Service.

Expanded Incident Lifecycle
Detailed stages in the lifecycle of an incident. The stages are detection, diagnosis, repair, recovery and restoration. The Expanded Incident Lifecycle is use to help understand all contributions to the impact of incidents and to plan for how these could be controlled or reduced.

External Customer
A Customer who works for a different Business than the IT Service Provider. See also External Service Provider.

External Metric
A Metric that is used to measure the delivery of IT Service to a Customer. External Metrics are usually defined in SLAs and reported to Customers. See also Internal Metric.

External Service Provider
An IT Service Provider that is part of a different Organization from its Customer. An IT Service Provider may have both Internal Customers and External Customers.

F

Facilities Management
The Function responsible for managing the physical Environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical Environment, for example power and cooling, building Access Management, and environmental Monitoring.

Failure
Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, Configuration Items, etc. A Failure often causes an Incident.

Fault
See Error.

Fault Tolerance
The ability of an IT Service or Configuration Item to continue to Operate correctly after Failure of a Component part. See also Resilience, Countermeasure.

Fault Tree Analysis (FTA)
A technique that can be used to determine the chain of events that leads to a Problem. Fault Tree Analysts represents a chain of events using Boolean notation in a diagram.

Financial Management
The Function and Processes responsible for managing an IT Service Provider's Budgeting, Accounting and Charging Requirements.

Financial Management for IT Services
The function and processes responsible for managing an IT Service Provider’s budgeting, accounting and charging requirements. Financial Management for IT Services secures an appropriate level of funding to design, develop and deliver services that meet the strategy of the organization in a cost-effective manner. See also Enterprise Financial Management.

First Line Support
The first level in a hierarchy of Support Groups involved in the resolution of Incidents. Each level contains more specialist skills, or has more time or other resources. See also Escalation.

Fishbone Diagram
See Ishikawa Diagram

Fit for Purpose
An informal term used to describe a Process, Configuration Item, IT Service, etc. that is capable of meeting its objectives or Service Levels. Being Fit for Purpose requires suitable design, implementation, control and maintenance.

Fit for Use
The ability to meet an agreed level of warranty. Being fit for use requires suitable design, implementation, control and maintenance.

Fixed Asset Management
The process responsible for tracking and reporting the value and ownership of fixed assets throughout their lifecycle. Fixed Asset Management maintains the asset register and is usually carried out by the overall business, rather than by the IT organization. Fixed Asset Management is sometime called Financial Asset Management and is not described in detail within the core ITIL publications.

Follow the Sun
A methodology for using Service Desks and Support Groups around the world to provide seamless 24/7 Service. Calls, Incidents, Problems and Service Requests are passed between groups in different time zones.

Fulfillment
Performing Activities to meet a need or Requirement. For example, by providing a new IT Service, or meeting a Service Request.

Function
A team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk. The team Function also ha two other meanings; an intended purpose of a Configuration Item, Person, Team, Process or IT Service. For example one Function of an e-mail Service may be to store and forward outgoing mails, one function of a Business Process may be to dispatch goods to Customers, and to perform the intended purpose correctly. The computer is Functioning.

Functional Escalation
Transferring an Incident, Problem or Change to a technical team with a higher level of expertise to assist in an Escalation.

G

Gap Analysis
An activity that compares two sets of data and identifies the differences. Gap Analysis is commonly used to compare a set of requirements with actual delivery. See also benchmarking.

Governance
Ensuring that Policies and Strategy are actually implemented and that required Processes are correctly followed. Governance includes defining Roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

Guideline
A Document describing Best Practice, which recommends what should be done. Compliance with a guideline is not normally enforced. See also standard.

H

Help Desk
A point of contact for Users to log Incidents. A Help Desk is usually more technically focused than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often used as a synonym for Service Desk.

Hierarchical Escalation
Informing or involving more senior levels of management to assist in an Escalation.

High Availability
An approach or design that minimizes or hides the effects of Configuration Item Failure on the Users of an IT Service. High Availability solutions are designed to achieve an agreed level of Availability and make use of techniques such as Fault Tolerance, Resilience and fast Recovery to reduce the number of Incidents, and the impact of incidents.

I

Identity
A unique name that is used to identify a User, person or Role. The identity is used to grant Rights to that User, person or Roles. Example identities might be the user name Smith or the Role 'Change Manager'.

Immediate Recovery
A Recovery Option that is also known as Hot Standby. Provision is made to recover the IT Service with no loss of Service. Immediate Recovery typically uses Mirroring, Load Balancing and Split Site technologies.

Impact
A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.

Incident
An unplanned interruption to an IT Service or reduction in the Quality of an IT Service Failure of a Configuration Item that has not yet affected service is also an incident. For example Failure of one disk from a mirror set.

Incident Management
The Process responsible for managing the Lifecycle of all incidents. The primary Objective of Incident Management is to return the IT Service to Customers as quickly as possible.

Incident record
A Record containing the details of an incident. Each Incident record documents the Lifecycle of a single Incident.

Indirect Cost
A cost of providing an IT Service, which cannot be allocated in full to a specific customer. For example, the cost of providing shared Servers or software Licenses. Also known as Overhead.

Information recovery
A Recovery Option that is also known as Warm Standby. Provision is made to Recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically uses a shared Portable or Fixed facility that has Computer Systems and Network Components. The hardware and software will need to be configured and data will need to be restored as part of the IT Service Continuity Plan

Information Security Management (ISM)
The Process that ensures the Confidentiality, Integrity, and Availability of an Organization’s Assets. Information, data and IT Services. Information Security Management usually forms part of an Organizational approach to Security Management that has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls, etc. for the entire Organization.

Information Security Management System (ISMS)
The framework of policy, processes, functions, standards guidelines, and tools that ensures an organization can achieve its Information Security Management objectives. See also Security Management Information System.

Information Security Policy
The Policy that governs the Organizations approach to Information Security Management.

Information Technology (IT)
The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Service.

Insourcing
See Internal Sourcing.

Integrity
A security principle that ensures data and Configuration Items are modified only by authorized personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events and human intervention.

Interactive Voice Response (IVR)
A form of Automatic Call Distribution that accepts User input such as key presses and spoken commands, to identify the correct destination for incoming calls.

Internal Customer
A customer who works for the same business as the IT Service Provider. See also External Customer; Internal Service Provider.

Internal Metric
A Metric that is used within the IT Service Provider to Monitor the Efficiency, Effectiveness or Cost Effectiveness of the IT Service Provider's internal Processes. Internal Metrics are not normally reported to the Customer of the IT Service. See Also External Metric.

Internal Rate of Return (IRR)
A technique used to help make decisions about capital expenditure. It calculates a figure that allows two or more alternative investments to be compared. A larger Internal Rate of Return indicates a better investment. See also Net Present Value; Return on Investment.

Internal Service Provider
An IT Service Provider that is part of the same Organization as its Customer. An IT Service Provider may have both Internal Customers and External Customers.

Internal Sourcing
Using an Internal Service Provider to manage IT Services.

International Organization for Standardization (ISO)
The International Organization for Standardization (ISO) is the world's largest developer of Standards. ISO is a non-governmental organization that is a network of the national standards institutes of 156 countries. See www.iso.org for further information about ISO.

Internet Service Provider (ISP)
An External Service Provider that provides access to the Internet. Most ISPs also provide other IT Services such as web hosting

Invocation
Initiation of the steps defined in a plan. For example initiating the IT Service Continuity Plan for one or more IT Services.

Ishikawa Diagram
A technique that helps a team to identify all the possible causes of a Problem. Originally devised by Kaoru Ishikawa, the output of this technique is a diagram that looks like a fishbone.

ISO 9000
A genetic term that refers to a number of international Standards and Guidelines for Quality Management System. See www.iso.org for more information. See also ISO.

ISO 9001
An international standard for quality management. See also ISO 9000

ISO/IEC 27001
An international specification for Information Security Management. The corresponding code of practices is ISO/IEC 27002. See also standard.

ISO/IEC20000
ISO Specification and Code of Practice for IT Service Management. ISO/IEC20000is aligned with ITIL Best Practice

IT Infrastructure
All of the hardware, software, networks, facilities, etc. that are required to develop, test, deliver, Monitor, Control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.

IT Operations
Activities carried out by IT Operations, Control, including Console Management. Job Scheduling, Backup and Restore, and Print and Output Management. IT Operations is also used as a synonym for Service Operation.

IT Operations Control
The function responsible for Monitoring and Control of the IT Services and IT Infrastructure. See also Operations Bridge.

IT Operations Management
The function within an IT Service Provider that performs the daily Activities needed to manage IT Services and the supporting IT Infrastructure. IT Operations Management includes IT Operations Control and Facilities Management.

IT Service
A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.

IT Service Continuity Management (ITSCM)
The Process responsible for managing Risks that could seriously affect IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.

IT Service Continuity Plan
A plan defining the steps required to Recover one or more IT Services. The plan will also identify the triggers for invocation, people to be involved, communications etc. The IT Service Continuity Plan should be part of a Business Continuity Plan

IT Service Management (ITSM)
The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management are performed by IT Service Providers through an appropriate mix of people, Process and Information Technology. See also Service Management.

IT Service Management Forum (itSMF)
The IT Service Management Forum is an independent Organization dedicated to promoting a professional approach to IT Service Management. The ITSMF is a not-for-profit membership Organization with representation in many countries around the world (ITSMF Chapters). The ITSMF and its membership contribute to the development of ITIL and associated IT Service Management Standards. See www.itsmf.com for more information.

IT Service Provider
A Service Provider that provides IT Services to internal or external customers.

ITIL
A set of Best Practice guidelines for IT Service Management. ITIL is owned by the OGC and consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See www.itil.co.uk for more information.

J

Job Description

A Document that defines the Roles, responsibilities, skills and knowledge required by a particular person. One Job Description can include multiple Roles, for example the Role of Configuration Manager and Change Manager may be carried out by one person.

K

Kempner Trego Analysis

Planning and managing the execution of software tasks that are required as part of an IT Service. Job Scheduling is carried out by IT Operations Management and is often automated using software tools that run batch or online tasks at specific times of the day, week, month or year.

Key Performance Indicator (KPI)

A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness and Cost Effectiveness are all managed. See also Critical Success Factor.

Knowledge Base

A logical database containing the data used by the Service Knowledge Management System.

Knowledge Management

The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge. See also Service Knowledge Management System.

Known Error

A Problem that has a documented Root Cause and a Workaround. Known errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may also be identified by Development or Suppliers.

Known Error Database (KEDB)

A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management. The known Error Database is part of the Service Knowledge Management system.

Known Error Record

A Record containing the details of a Known Error. Each Known Error Record documents the Lifecycle of a Known Error, including the Status, Root Cause and Workaround. In some implementations a Known Error is documented using additional fields in a Problem Record.

L

Lifecycle

The various stages in the life of an IT Service, Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. The Lifecycle of an Application includes Requirements, Design, Build, Deploy, Operate, Optimize. The Expanded Incident Lifecycle includes Detect, Respond, Diagnose, Repair, Recover, Restore. The Lifecycle of a Server may include: Ordered, received, In Test, Live, disposed, etc.

Live

Refers to an IT Service or Configuration Item that being used to deliver Service to a Customer.

Live Environment

A controlled Environment containing Live Configuration Items used to deliver IT Services to Customers.

M

Maintainability
A measure of how quickly and effectively an IT Service or other Configuration Item can be restored to normal working after a failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of software or IT Services development to mean ability to be changed or repaired easily.

Major Incident
The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Management Information
Information that is used to support decision making by managers. Management Information is often generated automatically by tools supporting the various IT Service Management Processes. Management Information often includes the values of KPIs such as Percentage of Changes leading to Incidents or first-time fix rate.

Management Information Systems (MIS)

Management of Risk (MoR)
The OGC methodology for managing Risks. MoR includes all the Activities requir4ed to identify and Control the exposure to Risk, which may have an impact on the achievement of an Organization's Business Objectives. See www.m-o-r.org for more details.

Management System
The framework of Policy, Processes and Functions that ensures an Organization can achieve its Objectives.

Manual Workaround
A workaround that requires manual intervention. Manual workaround is also used as the name of a recovery option in which the business process operates without the use of IT Services This is a temporary measure and is usually combined with another recovery option.

Market Space
Opportunities that an IT Service Provider could exploit to meet the business needs of customers. Market Spaces identify the possible IT Services that an IT Service Provider may wish to consider delivering.

Maturity
A measure of the reliability, efficiency and effectiveness of a process, function, organization tc. The most mature processes and functions are formally aligned to business objectives and strategy, and are supported by a framework for continual improvement.

Maturity Level
A named level in a maturity model, such as the Carnegie Mellon Capability Maturity Model Integration (CMMI).

Mean Time Between Failures (MTBF)
A Metric for measuring and reporting Reliability. MTBF is the average time that a Configuration Item or IT Service can perform its agreed Function without interruption. This is measured from when the CI or IT Service starts working, until it next fails.

Mean Time To Repair (MTTR)
The average time taken to repair a Configuration Item or IT Service after Failure. MTTR is measured from when the CI or IT Service fails until it is repaired. MTTR does not include the time required to Recover or Restore. MTTR is sometimes incorrectly used to mean Mean Time to Restore Service.

Mean Time to Restore Service (MTRS)
The average time taken to restore a Configuration Item or IT Service after a Failure. MTRS is measured from when the CI or IT Service fails until it is fully restored and delivering its normal functionality. See also Mean Time To Repair.

Metric
Something that is measured and reported to help manage a Process, IT Service or Activity. See also KPI

MIddleware
Software that connects two or more software Components or Applications. Middleware is

usually purchased from a Supplier, rather than developed within the IT Service Provider. See also Off the Shelf.

Mission
A short but complete description of the overall purpose and intentions of an organization. It states what is to be achieved, but not how this should be done. See also Vision.

Model
A representation of a System, Process, IT Service, Configuration Item, etc. that is used to help understand or predict future behavior.

Modeling
A technique that is used to predict the future behavior of a System, Process, IT Service, Configuration Item, etc. Modeling is commonly used in Financial Management, Capacity Management and Availability Management.

Monitor Control Loop
Monitoring the output of a Task, Process, IT Service or Configuration Item; comparing this output to a predefined Norm; and taking appropriate action based on this comparison.

Monitoring
Repeated observation of a Configuration Item, IT Service or Process to detect events and to ensure that the current status is known.

MyTerm

N

Net Present Value (NPV)
A technique used to help make decisions about capital expenditures. It compares cash inflows with cash outflows. Positive net present value indicates that an investment is worthwhile. See also Internal Rate of Return; Return on Investment.

O

Objective
The defined purpose or aim of a Process, an Activity or an Organization as a whole, Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement. See also Outcome.

Off the Shelf
See Commercial off the Shelf

Office of Government Commerce (OGC)
OGC (formater owner of Best Management Practice_ and its functins have moved into the Cabinet Office as part of HM Government. See www.cabinetoffice.gov.uk

Off-shore
Provision of Services from a location outside the country where the Customer is based, often in a different continent. This can be the provision of an IT Service or of supporting Functions such as Service Desk.

Operate
To perform as expected. A Process or Configuration Item is said to Operate if it is delivering the Required outputs. Operate also means to perform one or more Operations. For example, to Operate a computer is to do the day-to-day Operations needed for it to perform as expected.

Operation
Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.

Operational
The lowest of three levels of Planning and delivery. (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short-term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also a synonym for Live.

Operational Cost
Cost resulting from running the IT Services. Often repeating payments. For Example staff costs, hardware maintenance and electricity (also known as current expenditure or revenue expenditure). See also Capital Expenditure.

Operational Expenditure
See also Operational Cost

Operational Level Agreement (OLA)
An Agreement between an IT Service Provider and another part of the same organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example there could be an OLA between the IT Service Provider and a procurement department to obtain hardware that covers agreed-times. or between the Service Desk and a Support Group to provide Incident Resolution in agreed-times.

Operations Bridge
A physical location where IT Services and IT Infrastructure are monitored and managed

Operations Control
See also IT Operations Control

Operations Management
See also IT Operations Management

Optimize
Review, Plan and request Changes, in order to obtain the maximum Efficiency and Effectiveness from a Process, Configuration, Item, Application, etc.

Organization
A company, legal entity or other institution. Examples of Organizations that are not companies include International Standards Organization or ITSMF. The term Organization is sometimes used to refer to an entity that has People, Resources and Budgets. For example a Project or Business Unit.

Outcome
The result of carrying out an Activity; following a Process; delivering an IT Service, etc. The term Outcome is used to refer to intended results, as well as to actual results. See also Objective.

Outsourcing
Using an External Service Provider to manage IT Services. See also Service Sourcing.

Overhead
See indirect cost.

P

Pareto Principle
A technique use dot prioritize activities. The Pareto Principle says that 80% of the value of any activity is created with 20% of the effort. Pareto Analysis is also used in Problem Management to prioritize possible problem cause for investigation.

Partnership
A relationship between two Organizations that involves working closely together for common goals or mutual benefit. The IT Service Provider should have a Partnership with the Business, and with Third Parties who are critical to the delivery of IT Services.

Pattern of Business Activity (PBA)
A workload profile of one or more business activities. Patterns of Business Activity are used to help the IT Service Provider understand and plan for different levels of business activity. See also User Profile.

Performance
A measure of what is achieved or delivered by a System, person, team, Process, or IT Service.

Performance Management
The Process responsible for day-to-day Capacity Management Activities.. These include monitoring, threshold detection, Performance analysis and Tuning, and implementing changes related to Performance and Capacity.

Pilot
A limited Deployment of an IT Service, a Release or a Process to the Live Environment. A pilot is used to reduce Risk and to gain User feedback and Acceptance. See also Test, Evaluation.

Plan
A detailed proposal that describes the Activities and Resources needed to achieve an Objective. For example, a Plan to implement a new IT Service or Process. ISO/IEC 20000

requires a Plan for the management of each IT Service Management Process.

Plan-Do-Check-Act
A four stage cycle for Process management attributed to Edward Deming Plan. Do-Check-Act is also called the Deming Cycle.

Planning
An Activity responsible for creating one or more Plans. For example. Capacity Planning.

PMBOK
A Project Management Standard maintained and published by the Project Management Institute. PMBOK stands for Project Management Body of Knowledge. See www.pmi.org for more information. See also PRINCE2.

Policy
Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure, etc.

Post-Implementation Review (PIR)
A Review that takes place after a Change or a Project has been implemented. A PIR determines if the Change or Project was successful and identifies opportunities for improvement.

Practice
A way of working, or a way in which work must be done. Practices can include Activities, Processes, Functions, Standards and Guidelines. See also Best Practice.

Pricing
The Activity for establishing how much Customers will be Charged.

PRiNCE2
The standard UK government methodology for Project management. See www.ogc.gov.uk/prince2. See also PMBOK

Priority
A Category used to identify the relative importance of an incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority 2 Incidents must be resolved within 12 hours.

Proactive Problem Management
Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant problems.

Problem
A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.

Problem Management
The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent incidents from happening and to minimize the impact of Incidents that cannot be prevented.

Problem Record
A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.

Procedure
A Document containing steps that specify how to achieve an Activity. Procedures are defined as part of Processes. See also Word Instruction.

Process
A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities and Work Instruments if they are needed.

Process Control
The Activity of planning and regulating a Process, with the Objective of performing the

Process in an Effective, Efficient and consistent manner.

Process Manager
A Role responsible for Operational management of a Process. The Process Manager's responsibilities include planning and coordination of all Activities required to carry out, monitor and report on the process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data Centre. The Process Manager Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger Organizations.

Process Owner
A Role responsible for ensuring that a Process is Fit for Purpose The Process Owner's responsibilities include sponsorship, Design, Change Management and continual improvement of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organizations.

Production Environment
See Live Environment.

Program
A number of Projects and Activities that are planned and managed together to achieve an overall set of related Objectives and other Outcomes

Project
A temporary Organization, with people and other Assets required to achieve an Objective or other Outcome. Each Project has a Lifecycle that typically includes initiation, Planning, execution, Closure, etc. Projects are usually managed using a formal methodology such as PRiNCE2.

Project Management Body of Knowledge (PMBOK)
A project management standard maintained and published by the Project Management Institute.

Project Management Institute (PMI)
A membership association that advances the project management profession through globally recognized standards and certifications, collaborative communities, and extensive research program, and professional development opportunities. PMI is a not-for-for profit membership organization with representation in many countries around the world. PMI maintains and publishes the Project Management Body of Knowledge (PMBOK)

Project Management Office (PMO)
A function or group responsible for managing the lifecycle of projects. See also charter; project portfolio

Project Portfolio
A database or structure document used to manage projects throughout their lifecycle. The Project Portfolio is used to coordinate projects and ensure that they meet their objectives in a cost-effective and timely manner. In larger organizations, the Project Portfolio is typically defined and maintained by a Project Management Office. The Project Portfolio is important to Service Portfolio Management as new services and significant changes are are normally managed as projects. See also charter.

Projects IN Controlled Environments (PRiNCE2)
See PRiNCE2

Q

Qualification
An activity that ensures that IT infrastructure is appropriate, and correctly configured to support an Application or IT service. See also Validation.

Quality
The ability of a product, service or process to provide the intended value. For example, a hardware component can be considered to be of high quality if it performs as expected and delivers the required reliability. Process quality also requires an ability to monitor effectiveness and efficiency, and to improve them if

necessary. See also Quality Management System.

Quality Assurance (QA)
The process responsible for ensuring that the quality of a product, service or process will provide its intended value.

Quality Management System (QMS)
The set of processes responsible for ensuring that all work carried out by an organization is of a suitable quality to reliably meet business objectives or service levels. See also ISO 9000.

Quick Win
An improvement activity that is expected to provide a return on investment in a short period of time with relatively small cost and effort.

R

RACI
A model used to help define roles and responsibilities. RACI stands for Responsible, Accountable, Consulted and Informed.. See also Stakeholder

Record
A document containing the results or other output from a process or activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an audit report, an incident record or the minutes of a meeting.

Recovery
Returning a configuration item or an IT service to a working state. Recovery of an IT service often includes recovering data to a known, consistent state. After recovery, further steps may be needed before the IT service can be made available to the users. (Restoration).

Redundancy
See fault tolerance. The term redundant also has a generic meaning of obsolete or no longer needed.

Relationship
A connection or interaction between two people or things. In business relationship management it is the interaction between the IT service provider and the business. In configuration management it is a link between two configuration items that identifies a dependency or connection between them. For example applications may be linked to the servers they run on, IT services have many links to all the CIs that contribute to them.

Release
A collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to it services. The contents of each release are managed, tested, and deployed as a single entity.

Release & Deployment Management
The process responsible for both release management and deployment.

Release Management
The process responsible for planning, scheduling and controlling the movement of releases to test and live environments. The primary objective of release management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release management is part of the release and deployment management process.

Release Record
A record in the CMDB that defines the content of a release. A release record has relationships with all configuration items that are affected by the release.

Reliability
A measure of how long a configuration item or IT service can perform its agreed function without interruption. Usually measured as MTBF or MTBSI. The term reliability can also be used to state how likely it is that a process, function, etc. will deliver its required outputs. See also Availability.

Repair
The replacement or correction of a failed configuration item.

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.

Request Fulfillment
The process responsible for managing the lifecycle of all service requests.

Requirement
A formal statement of what is needed. For example, a service level requirement, a project requirement or the required deliverables for a process.

Resilience
The ability of a configuration item or IT service to resist failure or to recover quickly following a failure. For example an armored cable will resist failure when put under stress. See also Fault Tolerance.

Resolution
Action taken to repair the root cause of an incident or problem, or to implement a workaround. In ISO/IEC 20000, resolution processes is the process group that includes incident and problem management.

Resource
A generic term that includes IT infrastructure, people, money or anything else that might help to deliver an IT service, resources are considered to be assets of an organization. See also Capability, Service Asset.

Response Time
A measure of the time taken to complete an operation of transaction. Used in capacity management as a measure of IT infrastructure performance, and in incident management as a measure of the time taken to answer the phone or to start diagnosis.

Responsiveness
A measurement of the time taken to respond to something. This could be response time of a transaction, or the speed with which an IT service provider responds to an incident or request for change, etc.

Restoration Service
See Restore.

Restore
Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.

Retire
Permanent removal of an IT service, or other configuration item from the live environment. Retired is a state in the lifecycle of many configuration items.

Return on Investment (ROI)
Continual Service Improvement) A measurement of the expected benefit of an investment. In the simplest sense it is the net profit of an investment divided by the net worth of the assets invested. See also Value on Investments.

Review
An evaluation of a change, problem, process, project, etc. Reviews are typically carried out at pre-defined points in the lifecycle, and especially after closure. The purpose of a review is to ensure that all deliverables have been provided and to identify opportunities for improvement. See also Post-Implementation Review.

Risk
A possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.

Risk Assessment
The initial steps of risk management. Analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.

Risk Management
The process responsible for identifying, assessing and controlling risks. See also Risk Assessment.

Role
A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process. One person or team may have multiple roles, for example the roles of configuration manager and change manager may be carried out by a single person.

Root Cause
The underlying or original cause of an incident or problem.

Root Cause Analysis (RCA)
An activity that identifies the root cause of an incident or problem. RCA typically concentrates on IT infrastructure failures. See also Service Failure Analysis.

S

Sarbanes-Oxley (SOX)
US law that regulates financial practice and corporate governance.

Scalability
The ability of an IT service, process, configuration item, etc. to perform its agreed function when the workload or scope changes.

Scope
The boundary, or extent, to which a process, procedure, certification, contact, etc. applies. For example the scope of Change Management may include all live IT services and related configuration items, the scope of an ISO/IEC 20000 Certificate may include all IT services delivered out of a named data center.

Second Line Support
The second level in a hierarchy of support groups involved in the resolution of incidents and investigation of problems. Each level contains more specialist skills, or has more time or other resources.

Security
See Information Security Management

Security Management
See Information Security Management

Security Policy
See Information Security Policy

Server
A computer that is connected to a network and provides software functions that are used by other computers.

Service
A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Service Acceptance Criteria (SAC)
A set of criteria used to ensure that an IT Service meets its functionality and quality requirements and that the IT Service Provider is ready to operate the new IT Service when it has been deployed. See also Acceptance.

Service Asset
Any capability or resource of a service provider. See also Asset

Service Asset & Configuration Management (SACM)
The process responsible for both configuration management and asset management.

Service Capacity Management (SCM)
The activity responsible for understanding the performance and capacity of IT services. The resources used by each IT service and the pattern of usage over time are collected, recorded and analyzed for use in the capacity plan. See also Business Capacity Management, Component Capacity Management.

Service Catalog
A database or structured document with information about all live IT services, including those available for deployment. The service catalogue is the only part of the service portfolio published to customers, and is used to support the sale and delivery of IT services. The service catalogue includes information about deliverables, prices contact points, ordering and request processes.

Service Catalog Management
The process responsible for providing and maintaining the Service Catalog and for ensuring that it is available to those who are authorized to access it.

Service Charter
A document that contains details of a new or changed services. New service introductions and significant service changes are documented in a charter and authorized by Service Portfolio Management. Service Charters are passed to the Service Design lifecycle stage where a new or modified Service design Package will be created. The term charter is also used to describe the act of authorizing the work required by each stage of the service lifecycle with respect to the new or changed services. See also Change Proposal; Service Portfolio; Service Catalog.

Service Continuity Management
See IT service Continuity Management

Service Culture
A customer oriented culture. The major objectives of a service culture are customer satisfaction and helping customers to achieve their business objectives.

Service Design
A stage in the lifecycle of an IT service. Service design includes a number of processes and functions and is the title of one of the core ITIL publications. See also Design.

Service Design Package (SDP)
Documents defining all aspects of an IT Service and its requirements through each stage of its lifecycle. A Service Design Package is produced for each new IT Service, major change or IT Service retirement.

Service Desk
The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and also handles communication with the users.

Service Failure Analysis (SFA)
An activity that identifies underlying causes of one or more IT service interruptions. SFA identifies opportunities to improve the IT service providers processes and tools, and not just the IT infrastructure. SFA is a time constrained project-like activity, rather than an ongoing process of analysis. See also Root Cause Analysis.

Service Hours
An agreed time period when a particular IT service should be available. For example, 'Monday-Friday 09:00 to 17:00 except public holidays'. Service hours should be defined in a service level agreement.

Service Improvement Plan (SIP)
A formal plan to implement improvements to a process or IT service.

Service Knowledge Management System (SKMS)
A set of tools and databases that are used to manage knowledge and information. The SKMS includes the configuration management system as well as other tools and databases. The SKMS stores, manages, updates and presents all information that an ITservice provider needs to manage the full lifecycle of IT services.

Service Level
Measured and reported achievement against one or more service level targets. The team service level is sometimes used informally to mean service level target.

Service Level Agreements (SLA)
An agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers. See also Operational Level Agreement.

Service Level Management (SLM)
The process responsible for negotiating service level agreements and ensuring that these are met. SLM is responsible for ensuring that all IT service management processes, operation level agreements, and underpinning contracts, are appropriate for the agreed service level targets. SLM monitors and reports on service levels, and holds regular customer reviews.

Service Level Package
See Service Option.

Service Level Requirements (SLR)
A customer requirement for an aspect of an IT service. SLRs are based on business objectives and are used to negotiate agreed service level targets.

Service Level Target
A commitment that is documented in a service level agreement. Service level targets are based on service level requirements, and are needed to ensure that the IT service design is fit for purpose. Service level targets should be SMART, and usually based on KPIs.

Service Maintenance Objective
The expected time that a configuration item will be unavailable due to planned maintenance activity.

Service Management
Service management is a set of specialized organizational capabilities for providing value to customers in the form of services.

Service Management Lifecycle
An approach to IT Service Management that emphasizes the importance of coordination and control across the various function, processes and systems necessary to manage the full lifecycle of IT services. The Service Management Lifecycle approach considers the strategy, design, transition, operation and continuous improvement of IT services.

Service Manager
A manager who is responsible for managing the end-to-end lifecycle of one or more IT services. The term Service Manager is also used to mean any manager within the IT service provider. It is most commonly used to refer to a business relationship manager, a process manager, an account manager or a senior manager with responsibility for IT services overall.

Service Model
A model that shows how service assets interact with customer assets to create value. Service Models describe the structure of a service (how the configuration items fit together) and the dynamics of the service (activities, flow of resources and interactions). A Service Model can be used as a template or blueprint for multiple services.

Service Operation
A stage in the lifecycle of an IT service. Service Operation includes a number of processes and functions and is the title of one of the core ITIL publications. See also Operations.

Service Option
A choice of utility and warranty offered to customers by a core service or service package. Service Options are sometimes referred to as Service Level Packages.

Service Owner
A role responsible for managing one or more services throughout their entire lifecycle. Service Owners are instrumental in the development of Service Strategy and are responsible for the content of the Service Portfolio. See also Business Relationship Management.

Service Package
Two or more services that have been combine to offer a solution to a specific type of customer need or to underpin specific business outcomes. A Service Package can consist of a combination of core services, enabling services and enhancing services. A Service Package provides a specific level of utility and warranty. Customers may be offered a choice of utility and warranty through one or more service options. See also IT Service.

Service Pipeline
A database or structured document listing all IT Services that are under consideration or development, but are not yet available to customers. The Service pipeline provides a business view of possible future IT Services and is part o the Service Portfolio that is not normally published to customers.

Service Portfolio
The complete set of services that are managed by a service provider. The Service Portfolio is used to manage the entire lifecycle of all services and includes three categories, service pipeline (proposed or in development), service catalogue (live or available for

deployment) and retired services. See also Service Portfolio Management.

Service Portfolio Management (SPM)
The process responsible for managing the service portfolio. Service portfolio management considers service in terms of the business value that they provide.

Service Provider
An organization supplying services to one or more internal customers or external customers. Service Provider is often used as an abbreviation for IT Service Provider.

Service Reporting
The process responsible for producing and delivering reports of achievement and trends against service levels. Service Reporting should agree the format, content and frequency of reports with customers.

Service Request
A request from a user for information, or advice, or for a standard change or for access to an IT service. For example to reset a password, or to provide standard IT services for a new user. Service Requests are usually handled by a Service Desk and do not require an RFC to be submitted. See also Request Fulfillment.

Service Sourcing
The strategy and approach for deciding whether to provide a service internally, to outsource it to an external Service Provider, or to combine the two approaches. Service Sourcing also means the execution of this strategy. See also Insourcing; Internal Service Provider; Outsourcing.

Service Strategy
The title of one of the core ITIL publications. Service Strategy establishes an overall strategy for IT Services and for IT Service Management.

Service Transition
A stage in the lifecycle of an IT Service. Service Transition includes a number of processes and functions and is the title of one of the Core ITIL publications. See also Transition.

Service Validation and Testing
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.

Serviceability
The ability of a third-party supplier to meet the terms of its contract. This contract will include agreed levels of reliability, maintainability and availability for a Configuration Item.

Seven-step Improvement Process
The process responsible for defining and managing the steps needed to identify, define, gather, process, analyze, present and implement improvements. The performance of the IT Service Provider is continually measured by this process and improvements are made to processes, IT Service and IT infrastructure in order to increase efficiency, and effectiveness and cost effectiveness. Opportunities for improvement are recorded and managed in the CSI Resister.

Shift
A group or team of people who carry out a specific role for a fixed period of time. For example there could be four shifts of IT Operations Control personnel to support an IT service that is used 24 hours a day.

Simulation Modeling
A technique that creates a detailed model to predict the behavior of an IT Service or other Configuration Item. A Simulation Model is often created by using the actual Configuration Items that are being modeled with artificial workloads or transactions. They are used in Capacity Management when accurate results are important. A Simulation Model is sometimes called a performance benchmark. See also Analytical Modeling; modeling

Single Point of Contact
Providing a single consistent way to communicate with an organization or business unit. For example, a single point of contact for an IT service provider is usually called a service desk.

Single Point of Failure (SPOF)
Any Configuration Item that can cause an incident when it fails, and for which a countermeasure has not been implemented. A SPOF may be a person or a step in a process or activity, as well as a component of the IT infrastructure. See also Failure.

SLAM Chart
A Service Level Agreement Monitoring chart is used to help monitor and report achievements against Service Level Targets. A SLAM chart is typically color-coded to show whether each agreed Service Level Target has been met, missed or nearly missed during each of the previous 12 months.

SMART
An acronym for helping to remember that targets in Service Level Agreements and project plans should be Specific, Measurable, Achievable, Relevant and Time-bound

Software Asset Management (SAM)
The process responsible for tracking and reporting the use and ownership of software assets throughout their lifecycle. Software Asset Management is part of an overall Service Asset and Configuration Management process. This process is not described in detail with the core ITIL publications.

Source
See Service Sourcing.

Specification
A formal definition of requirements. A specification may be used to define technical or operational requirements, and may be internal or external. Many public standards consist of a code of practice and a specification. The specification defines the standard against which an organization can be audited.

Stakeholder
All people who have an interest in an organization, project, IT service, etc. Stakeholders may be interested in the activities, targets, resources or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, etc.

Standard
A mandatory requirement. Examples include ISO/IEC 20000 (an international standard), an internal security standard for Unix configuration, or a government standard for how financial records should be maintained. The term standard is also used to refer to a code of practice or specification published by a standards organization such as ISO or BSI. See also Guideline.

Standard Change
A pre-approved change that is low risk, relatively common and follows a procedure or work instruction. For example, password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a service request. See also Change Model

Standard Operating Procedures (SOP)
Procedures used by IT Operations Management.

Standby
Used to refer to resources that are not required to deliver the live IT services but are available to support IT Service Continuity plans. For example a standby data center may be maintained to support hot standby, warm standby or cold standby arrangements.

Statement of Requirements (SOR)
A document containing all requirements for a product purchase or a new or changed IT service.

Status
The name of a required field in many types of record. It shows the current stage in the lifecycle of the associated Configuration Item, Incident, Problem etc.

Storage Management
The process responsible for managing the storage and maintenance of data throughout its lifecycle.

Strategic
The highest of three levels of Planning and Delivery (Strategic, Tactical, Operational). Strategic activities include objective setting

and long term planning to achieve the overall vision.

Strategic Asset
Any asset that provides the basis for core competence, distinctive performance or sustainable competitive advantage, or which allows a business unit to participate in business opportunities. Part of Service Strategy is to identify how IT can be viewed as a strategic asset rather than an internal administrative function.

Strategy
A strategic plan designed to achieve defined objectives.

Strategy Management for IT Services
The process responsible for defining and maintaining an organization's perspective, position, plans and patterns with regard to its services and the management of those services. Once the strategy has been defined, Strategy Management for IT Services is also responsible for ensure that it achieves its intended business outcomes.

Super User
A user who helps other users, and assists in communication with the Service Desk or other parts of the IT Service Provider. Super users typically provide support for minor Incidents and training.

Supplier
A third party responsible for supplying goods or services that are required to deliver IT Services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing organizations. See also Underpinning Contract, Supply Chain.

Supplier and Contract Management Information System (SCMIS)
A set of tools, data and information that is used to support Supplier Management. See also Service Knowledge Management System.

Supplier Management
The process responsible for ensuring that all contracted with suppliers support the needs of the business, and that all Suppliers meet their contractual commitments.

Supply Chain
The activities in a value chain carried out by suppliers. A supply chain typically involves multiple suppliers, each adding value to the product or service. See also Value Network.

Support Group
A group of people with technical skills. Support groups provide the technical support needed by all of the IT Service Management processes. See also Technical Management.

Supporting Service
An IT Service that is not directly used by the business, but is required by the IT Service Provider to deliver customer-facing services. All live Supporting Services, including those available for deployment, are recorded in the Service Catalog along with information about their relationships to customer-facing services and other CIs.

SWOT Analysis
A technique that reviews and analyzes the internal strengths and weakness of an organization and the external opportunities and threats that if faces. SWOT stands for Strengths, Weaknesses, Opportunities, and Threats.

System
A number of related things that work together to achieve an overall objective. For example; a computer system, including hardware, software and applications, a management system, including multiple processes that are planned and managed.

T

Tactical
The middle of three levels of Planning and Delivery (Strategic, Tactical, Operational). Tactical activities include the medium-term plans required to achieve specific objectives, typically over a period of weeks to months.

Technical Management
The function responsible for providing technical skills in support of IT Services and management of the IT infrastructure. Technical management defines the roles of support groups, as well as the tools, processes and procedures required.

Technical Observation
A technique used in Service Improvement, Problem investigation and Availability Management. Technical support staff meet to monitor the behavior and performance of an IT service and make recommendations for improvement.

Technical Support
See Technical Management

Tension Metrics
A set of related metrics, in which improvements to one metric have a negative effect on another. Tension metrics are designed to ensure that an appropriate balance is achieved.

Terms of Reference (TOR)
A document specifying that requires, scope, deliverables, resources and schedule for a project or activity.

Test
An activity that verifies that a Configuration Item, IT Service, process, etc. meets its specification or agreed requirements.

Test Environment
A controlled environment used to test Configuration Items, builds, IT services, processes etc.

Third Party
A person, group, or business that is not part of the Service Level Agreement for an IT Service, but is required to ensure successful delivery of that IT Service. For example, a software supplier, a hardware maintenance company, or a facilities department. Requirements for third parties are typically specified in Underpinning Contracts or Operational Level Agreements.

Third-Line Support
The third level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other resources.

Threat
Anything that might explore a vulnerability. Any potential cause of an Incident can be considered to be a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability Management.

Threshold
The value of a metric that should cause an alert to be generated or management action to be taken. For example 'Priority 1 Incident not solved within four hours', 'more than five soft disk errors in an hour' or more than 10 failed changes in a month.

Throughput
A measure of the number of transactions, or other operations, performed in a fixed time for example. 5,000 e-mails sent per hour, or 200 disk I/Os per second.

Total Cost of Ownership
A methodology use to help make investment decisions. IT assesses the full lifecycle cost of owning a Configuration Item, not just the initial cost or purchase price. See also Total Cost of Utilization.

Total Cost of Utilization (TCU)
A methodology used to help make investment and service sourcing decisions. Total Coast of Utilization assesses the full lifecycle cost to the customer of using an IT Service. See also Total Cost of Ownership.

Total Quality Management (TQM)
A methodology for managing continual improvement by using a Quality Management System. TQM establishes a culture involving all people in the organization in a process of continual monitoring and improvement.

Transaction
A discrete function performed by an IT Service. For example transferring money from one bank account to another. A single transaction may involve numerous additions, deletions an modifications of date. Either all of these complete successfully or none of them carried out.

Transition
A change in state, corresponding to a movement of an IT Service or other Configuration Item from one lifecycle status to the next.

Transition Planning and Support
The process responsible for planning all Service Transition processes and coordinating the resources that they require.

Trend Analysis
Analysts of data to identify time-related patterns. Trend Analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modeling tool to predict future behavior. It is also used as a management tool for identifying deficiencies in IT Service Management processes.

Tuning
The activity responsible for planning changes to make the most efficient use of resources. Tuning is part of Performance Management, which also includes performance monitoring and implementation of the required changes.

Type I Service Provider
An internal Service Provider that is embedded within a business unit. There may be several Type I Service Providers within an organization.

Type II Service Provider
An internal Service Provider that provides shared IT Services to more than one business unit. Type II Service Providers are also known as shared service units.

Type III Service Provider
A Service Provider that provides IT Services to external customers.

U

Underpinning Contract (UC)
A contract between an IT Service provider and a third party. The third party provides goods or services that support delivery of an IT Service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.

Unit Cost
The cost to the IT Service Provider of providing a single component of an IT service. For example, the cost of a single desktop PC, or of a single transaction.

Urgency
A measure of how long it will be until an Incident, Problem or Change has a significant impact on the business. For example a high impact Incident may have low Urgency, if the impact will not affect the business until the end of the financial year. Impact and Urgency are used to assign Priority.

Usability
The ease with which an application, product or IT Service can be used, Usability Requirements are often included in a Statement of Requirements.

Use Case
A technique used to define required functionality and objectives, and to design tests. Use Cases define realistic scenarios that describe interactions between Users and an IT Service or other system. See also Change Case.

User
A person who uses the IT Service on a day- to-day basis. Users are distinct from Customers as some Customers do not use the IT Service directly.

User Profile (UP)
A pattern of User demand for IT Services. Each User profile includes one or more patterns of business activity.

Utility
Functionality offered by a product or service to meet a particular need. Utility is often summarized as what it does.

V

Validation
An activity that ensures a new or changed IT Service, process, plan or other deliverable meets the needs of the business. Validation ensures that business requirements are met even though these may have changed since the original design. See also Verification, Acceptance or Qualification.

Value Chain
A sequence of processes that creates a product or service that is of value to a customer. Each step of the sequence builds on the previous steps and contributes to the overall product or service. See also Value Network.

Value for Money
An informal measure of cost effectiveness. Value for money is often based on a comparison with the cost of alternatives.. See also Cost Benefit Analysis.

Value Network
A complex set of relationships between two or more groups or organizations. Value is generated through exchange of knowledge, information, goods or services. See also Partnership; Value Chain.

Value on Investment (VOI)
A measurement of the expected benefit of an investment. Value on Investment considers both financial and intangible benefits. See also Return on Investment.

Variance
The difference between a planned value and the actual measured value. Commonly used in Financial Management, Capacity Management and Service Level Management, but could apply in any area where plans are in place.

Verification
An activity that ensures a new or changed IT service, process, plan or other deliverable is complete, accurate, reliable and matches its design specification. See also Validation, Acceptance.

Version
A description of what the organization intends to become in the future. A vision is created by senior management and is used to help influence culture and strategic planning.

Vision
A description of what the organization intends to become in the future. A vision is created by senior management and is used to help influence culture and strategic planning. See also Mission.

Vital Business Function (VBF)
A function of a business process that is critical to the success of the business. Vital business functions are an important consideration of Business Continuity Management, IT Service Continuity Management and Availability Management.

Vulnerability
A weakness that could be exploited by a threat. A missing control is also considered to be a vulnerability.

W

Warranty
Assurance that a product or service will meet agreed requirements. This may be a formal agreement such as a Service Level Agreement or contract, or it may be a marketing message or brand image. Warranty refers to the ability of a service to be available when needed to provide the required capacity, and to provide the required reliability in terms of continuity and security. Warranty can be summarized as “how the service is delivered,” and can be used to determine whether a service is “fit for use.” The business value of an IT Service is created by the combination of utility and warranty. See also Service Validation and Testing.

Work in Progress (WIP)
A status that means activities have started but are not yet complete. It is commonly used as a status for Incidents, Problems, Changes, etc.

Work Instruction
A document containing detailed instructions that specify exactly what steps to follow to carry out an activity. A Work Instruction contains much more detail than a Procedure and is only created if very detailed instructions are needed.

Workaround
Reducing or eliminating the impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item, Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.

Workload
The resources required to deliver an identifiable part of an IT Service. Workloads may be categorized by users, groups of users or functions within the IT Service. This is used to assist in analyzing and managing the Capacity, Performance and Utilization of Configuration Items and IT Services. The term Workload is sometimes used as a synonym for Throughput.