SERVICE MANAGEMENT PRACTICES

Section 12

SERVICE MANAGEMENT PRACTICES

SERVICE MANAGEMENT PRACTICES

- Availability Management
- Business Analysis
- Capacity and Performance Management
- Change Enablement
- Incident Management
- IT Asset Management
- Monitoring and Event Management
- Problem Management
- Release Management
- Service Catalogue Management
- Service Configuration Management
- Service Continuity Management
- Service Design
- Service Desk
- Service Level Management
- Service Request Management
- Service Validation and Testing

MONITORING & EVENT MANAGEMENT

Monitoring And Event Management

to ensure the services and service components are observed systematically, detect & report the change of state which has significance to service, service performance, and contribution to the business

This practice identifies and prioritizes infrastructure, services, business processes, and information security events, and establishes the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents

MONITORING & EVENT MANAGEMENT

Event

any change of state that has significance for the management of a service or other configuration item (CI)

- **Events** are typically recognized through notifications created by an IT service, CI, or monitoring tool

- Manages events throughout their lifecycle to prevent, minimize, or eliminate their negative impact on the business

MONITORING & EVENT MANAGEMENT

Event Management https://www.youtube.com/watch?v=_-T29YZE5Qs

Monitoring

- **Focuses** on the **systematic observation** of services and the CIs that underpin services to detect conditions of potential significance
- **Monitoring** should be performed in a highly automated manner and can be done actively or passively
- **Monitoring** is necessary for event management to take place, but not all monitoring results in the detection of an event

Event

- **Events** are often classified as **informational**, **warning**, and **exceptions**
- **Informational events** do not require action when they are identified
- **Warning events** allow action to be taken before the business experiences any negative impact
- In contrast, **exception events** indicate that a breach of an established norm has been identified
- **Exception events** require action, even though business impact may not yet have been experienced

Activities

- **Identifying** what services, systems, cis, or other service components should be monitored
- **Implementing** and maintaining monitoring
- **Establishing and maintaining** thresholds and other criteria for determining which changes of state will be treated as events
- **Establishing and maintaining** policies for how each type of detected event should be handled to ensure proper management
- **Implementing processes** and automations required to operationalize the defined thresholds, criteria, and policies

MONITORING & EVENT MANAGEMENT

- This practice is highly **interactive** with other practices participating in the service value chain
- The **correct control** action will be to initiate activity in the incident management practice
- **Repeated events** showing performance outside of desired levels may be evidence of a potential problem, which would initiate activity in the problem management practice
- For some events, the **correct response** is to initiate a change, engaging the change control practice

MONITORING & EVENT MANAGEMENT

- Organizations and people are also critical to appropriately responding to monitored data and events aligned with policies and organizational priorities
- **Roles and responsibilities** must be clearly defined, and each person or group must have easy, timely access to the information needed to perform their role
- **Automation** is key to successful monitoring and event management
- The **monitoring** itself can be either active or passive
- In active **monitoring**, tools will poll key CIs, looking at their status to generate alerts when an exception condition is identified
- In passive **monitoring**, the CI itself generates the operational alerts

MONITORING & EVENT MANAGEMENT

- **Automated tools** should also be used for the correlation of events
- These features may be provided by monitoring tools or other tools such as **ITSM workflow systems**
- There can be a huge volume of data generated by this practice, but it will be of no value without clear policies and strategies on how to limit, filter, and use this data
- Don’t ask for data that is not truly needed, but if data is required, make sure that the provision of that data is explicitly part of the contract for the supplier’s services

MONITORING & EVENT MANAGEMENT

The difference between monitoring and event management

Monitoring and event management are closely related, but slightly different in nature. Event management is focused on generating and detecting meaningful notifications about the status of the IT infrastructure and services.

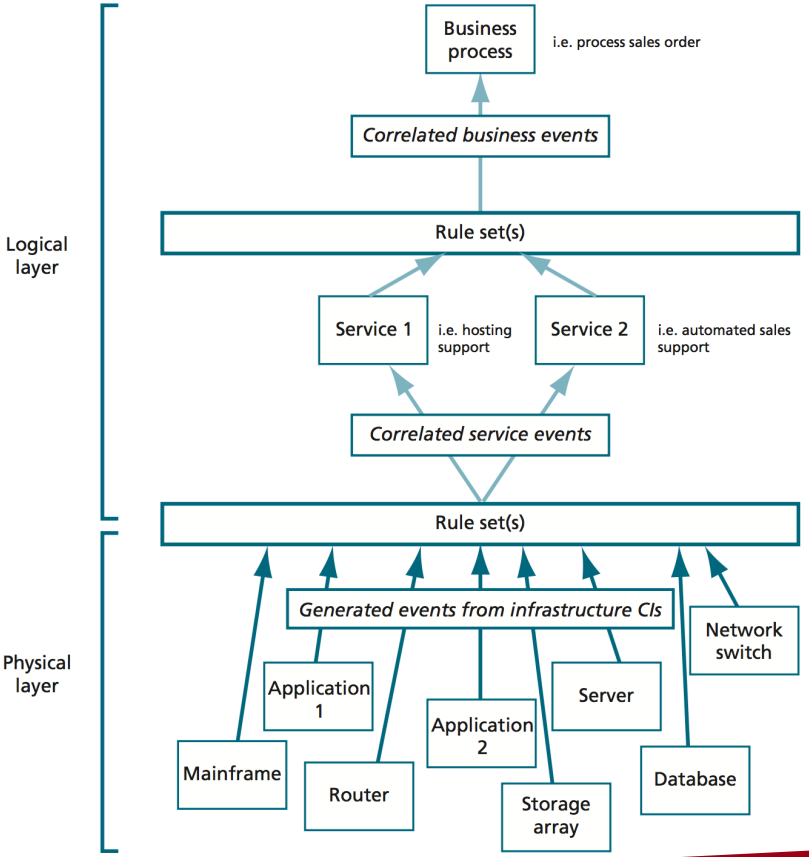
While it is true that monitoring is required to detect and track these notifications, monitoring is broader than event management. For example, monitoring tools will check the status of a device to ensure that it is operating within acceptable limits, even if that device is not generating events.

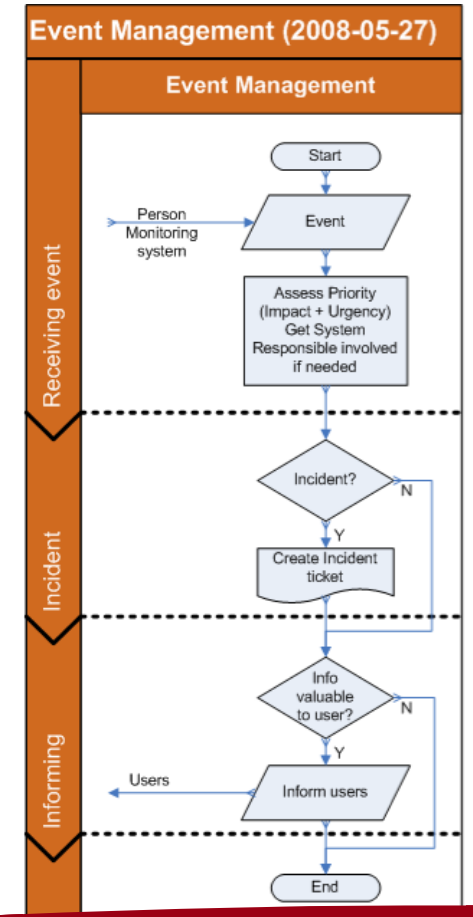
Put more simply, event management works with occurrences that are specifically generated to be monitored. Monitoring tracks these occurrences, but it will also actively seek out conditions that do not generate events.

Active versus passive monitoring

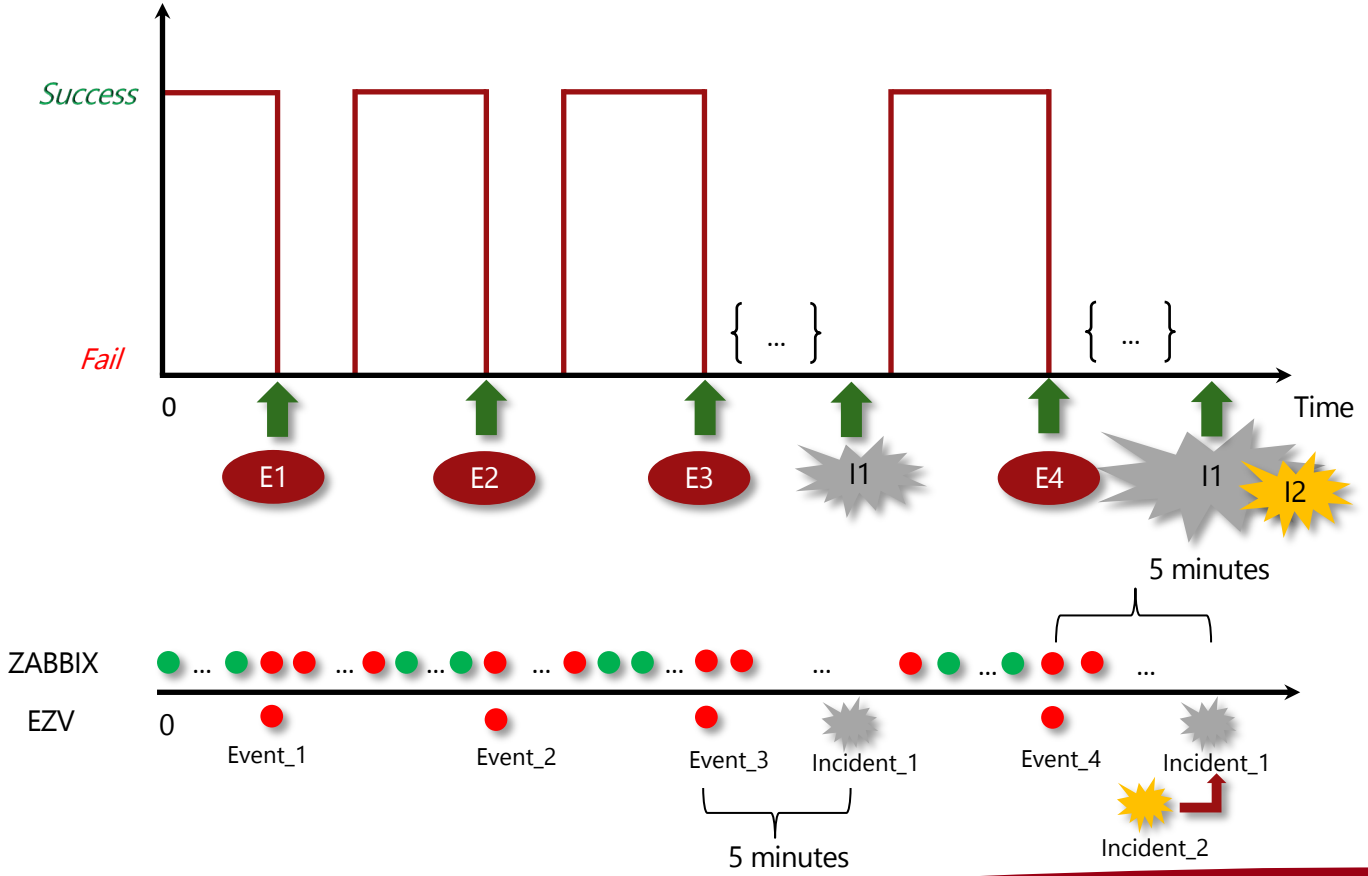
	Active	Passive
Reactive	Used to diagnose which device is causing the failure and under what conditions (e.g. 'ping' a device, or run and track a sample transaction through a series of devices) Requires knowledge of the infrastructure topography and the mapping of services to CIs Requires capability to simulate service workloads and demand volumes	Detects and correlates event records to determine the meaning of the events and the appropriate action (e.g. a user logs in three times with the incorrect password, which represents a security exception and is escalated through information security management procedures) Requires detailed knowledge of the normal operation of the infrastructure and services
Proactive	Used to determine the real-time status of a device, system or service – usually for critical components or following the recovery of a failed device to ensure that it is fully recovered (i.e. is not going to cause further incidents)	Event records are correlated over time to build trends for proactive problem management Patterns of events are defined and programmed into correlation tools for future recognition

MONITORING & EVENT MANAGEMENT

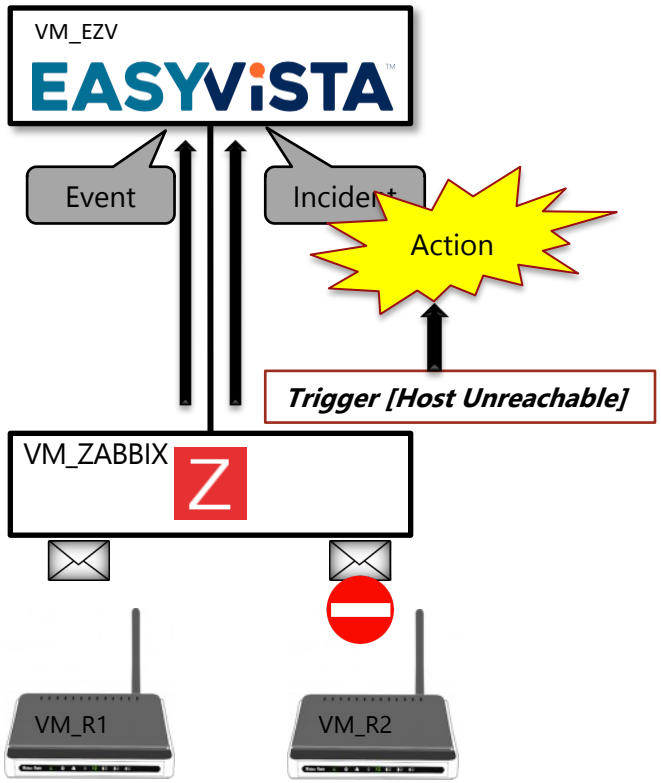




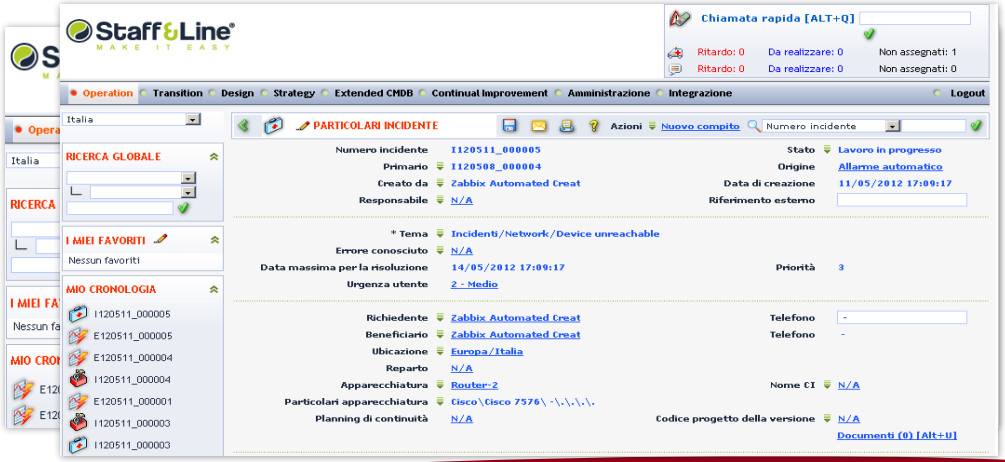
MONITORING & EVENT MANAGEMENT



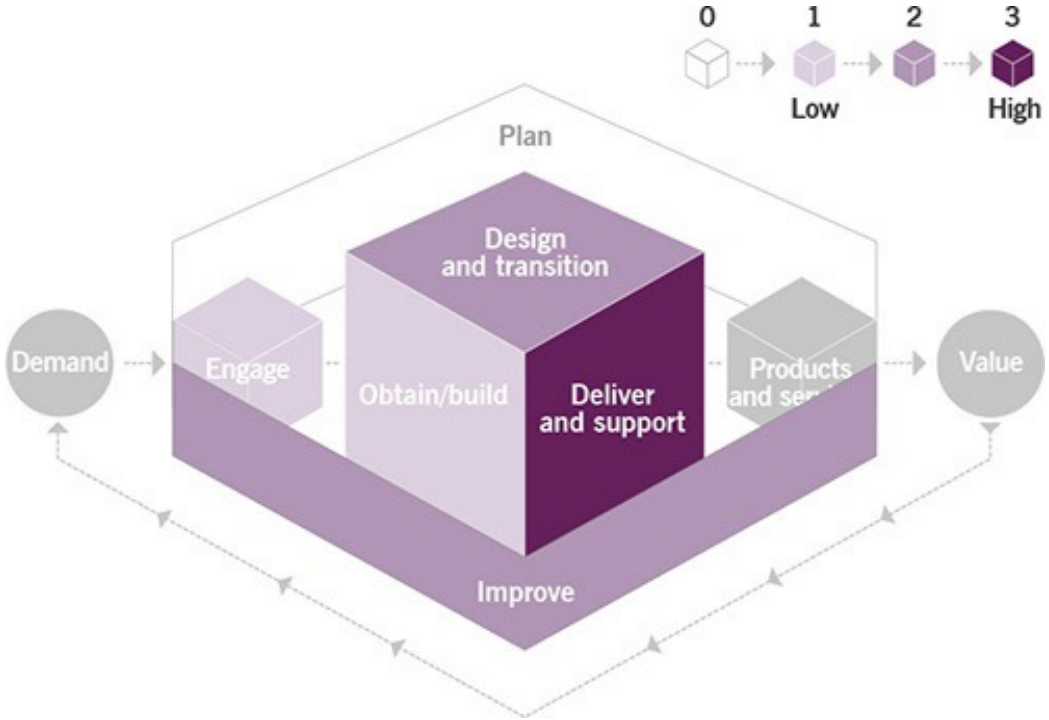
MONITORING & EVENT MANAGEMENT



1. *Active Monitoring*
2. Event: VM_R2 shutdown
3. Zabbix detects that the VM_R2 router is not reachable anymore
4. Execution of the action associated with the trigger
5. New event raised up on EasyVista
6. New incident raised up on EasyVista



MONITORING & EVENT MANAGEMENT



Heat map of the contribution of monitoring & event management to value chain activities

MONITORING & EVENT MANAGEMENT

Plan	Uninvolved
Improve	Essential to the close observation of the environment to evaluate and proactively improve its health and stability
Engage	Essential to the close observation of the environment to evaluate and proactively improve its health and stability
Design & Transition	Monitoring data informs design decisions Monitoring is an essential component of transition
Obtain / Build	Supports development environments, ensuring their transparency and manageability
Deliver & Support	The practice guides how the organization manages internal support of identified events, initiating other practices as appropriate

Incident Management

minimalizing the negative impact of incidents by restoring normal service operation as quickly as possible

INCIDENT MANAGEMENT

ITIL Journey - The Incident https://youtu.be/8cctLnKdEfo

Incident

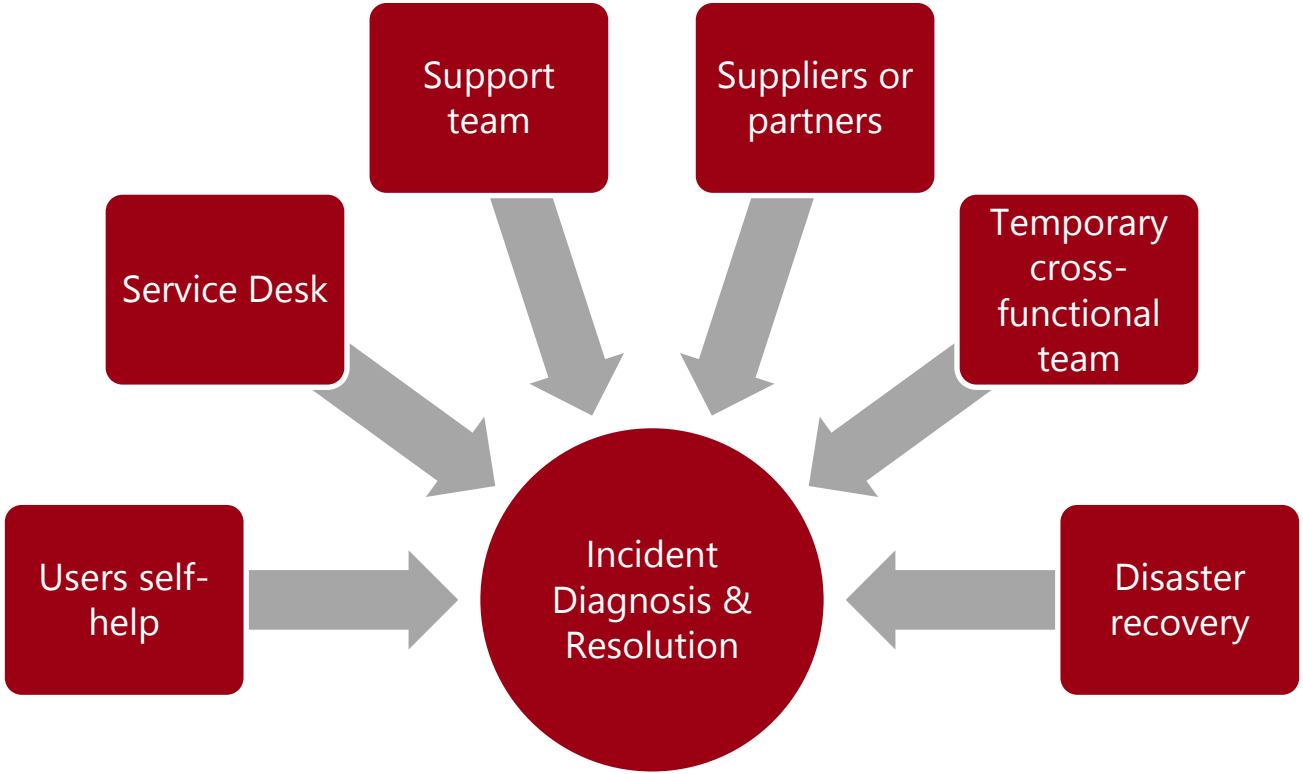
the unplanned interruption to a service or degradation of the service performance or quality

Swarming

involves many different stakeholders working together initially, until it becomes very clear which of them is best placed to continue and who can move on to other tasks

- Solving incidents relies heavily on collaboration and information sharing

INCIDENT MANAGEMENT



Classification

Classifying means assigning Priority and Category

Priority

- The SD determines the priority of incidents as soon as they are received
- The priority is established according to the criteria described in the SLA
- The priority is calculated on the basis of impact and urgency

Impact

effect that the incident has on business activities

Urgency

speed at which the incident must be resolved

The Impact is always intended as Business Impact

- Critical period (i.e. night or day?)
- Critical applications
- Number of users
- Etc.

When determining the priority, the following must be considered:

- The potential costs of non-resolution
- The threat of harm to customers and staff
- The legal implications
- The "nuisance" caused to customers and staff

The impact is not related to the technical complexity of the resolution

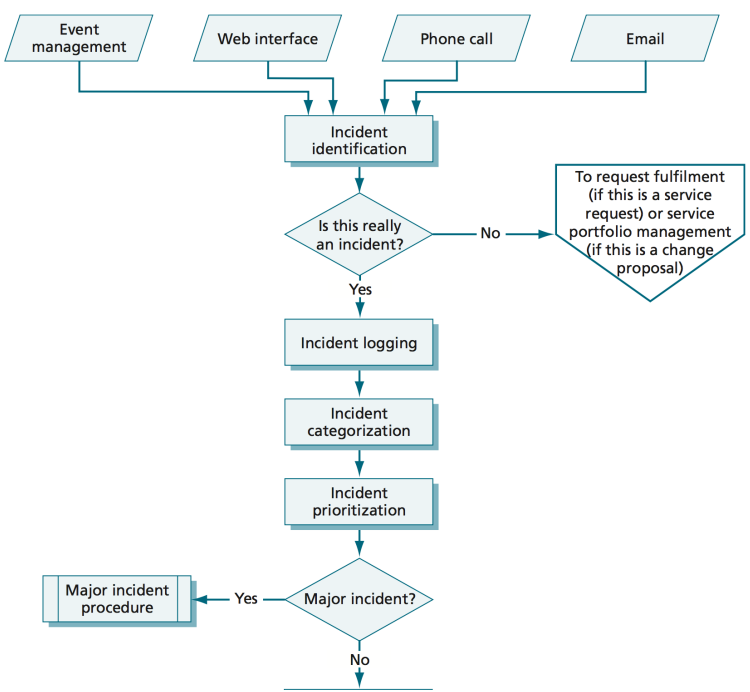
	Impact		
Urgency	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

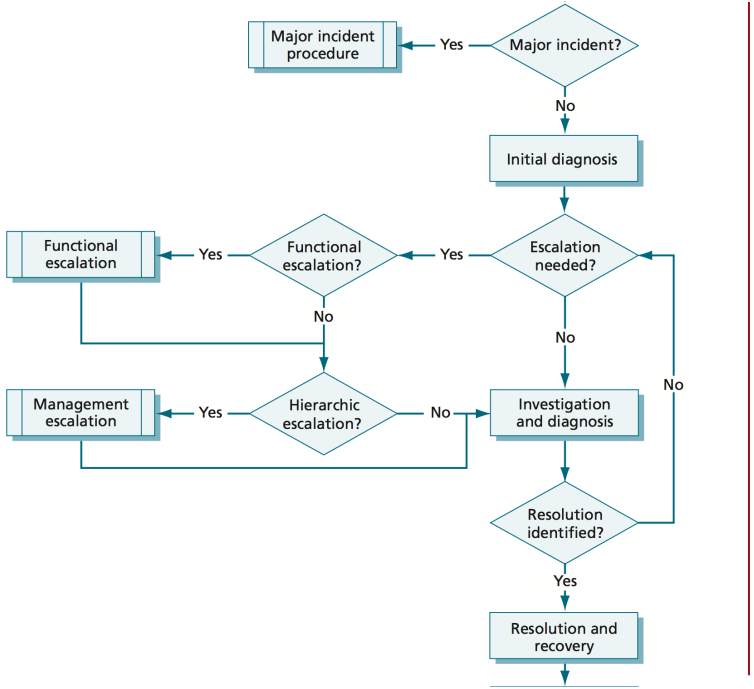
Priority code	Description	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

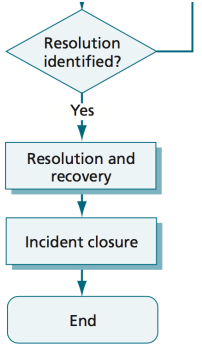
Hierarchical Escalation = Inform / Support
Functional Escalation = Knowledge

Escalation and Referral NEVER turn an incident into a problem, even when the owner of an incident speaks to the PM for administrative reasons, and the PM should proceed with the identification of an associated problem

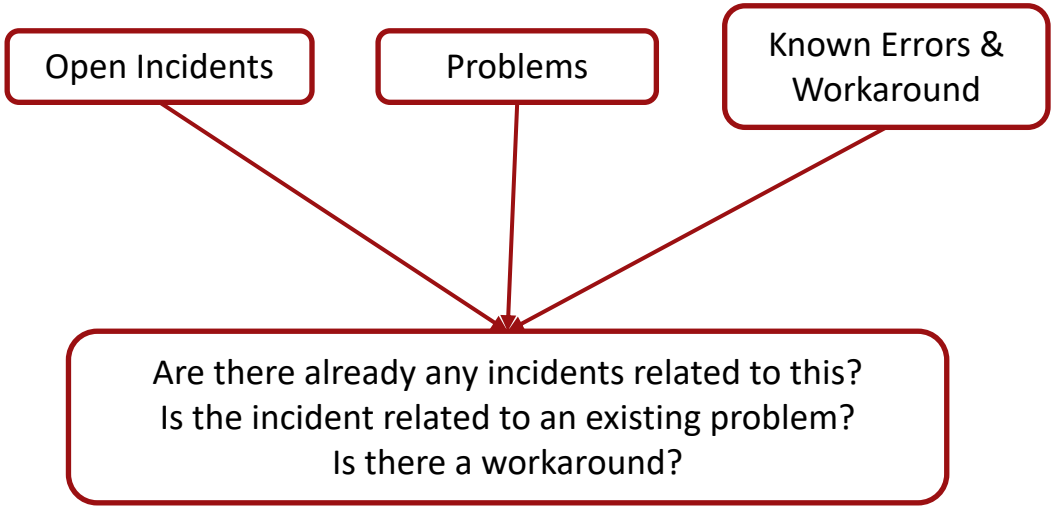
Problems are NOT serious accidents


Event management
Web interface
Phone call
Email
Incident identification
Is this really an incident?
No
To request fulfilment (if this is a service request) or service portfolio management (if this is a change proposal)
Yes
Incident logging
Incident categorization
Incident prioritization
Major incident procedure
Yes
Major incident?
No


Major incident procedure
Yes
Major incident?
No
Initial diagnosis
Functional escalation
Yes
Functional escalation?
Yes
Escalation needed?
No
No
Management escalation
Yes
Hierarchic escalation?
No
Investigation and diagnosis
No
Resolution identified?
Yes
Resolution and recovery


Resolution identified?
Yes
Resolution and recovery
Incident closure
End

Incident Matching

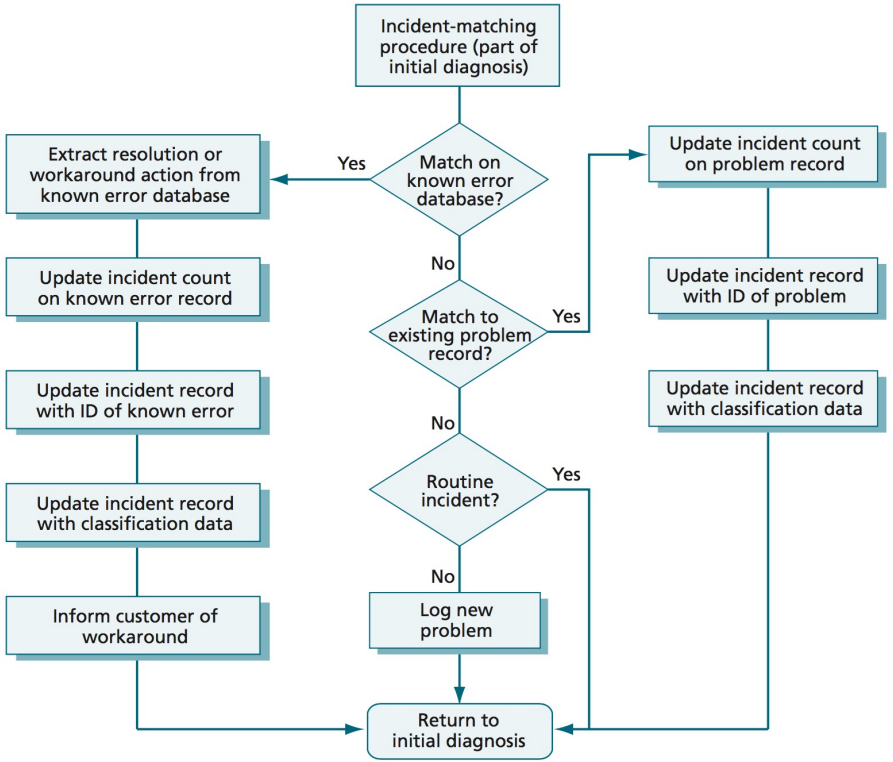


Incident matching procedure

Many incidents are regularly experienced and the appropriate resolution actions are well known. However, it is necessary to have a procedure for matching incident classification data against that for problems and known errors. Successful matching gives efficient and quick access to proven resolution actions, reducing the time it takes to restore service back to users. The process of classification and matching allows incident management to be carried out more quickly and minimizes the need for escalation to other support staff.

Effective use of incident matching ensures that incidents are not redundantly being investigated for resolution over and over each time. A procedure can be developed to help service desk and other support staff match incidents to find resolutions quickly where possible. An example of an incident-matching procedure is shown in Figure 4.5.

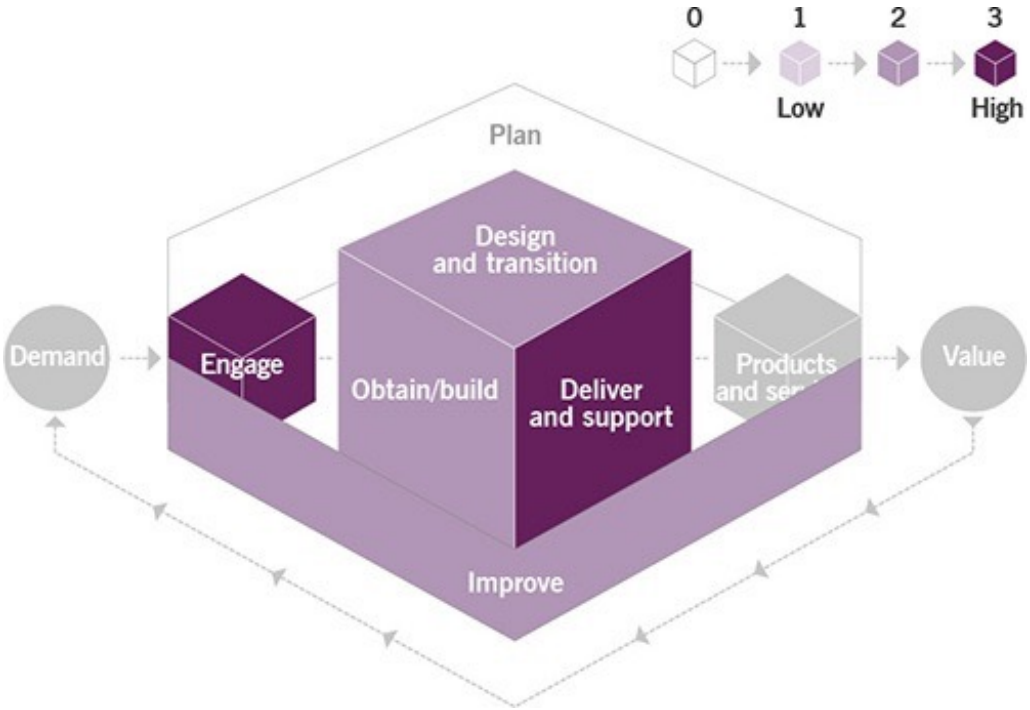
Incident Matching workflow



INCIDENT MANAGEMENT

Incident Management https://www.youtube.com/watch?v=q3xI97i1kkE

INCIDENT MANAGEMENT



Heat map of the contribution of incident management to value chain activities

INCIDENT MANAGEMENT

Plan	Uninvolved
Improve	improvement by reducing the incident resolution time, improving the user experience…etc
Engage	Engaging, coordination & communication with the users and subject matter expertise
Design & Transition	Resolving the incident which would occur during the design and transition
Obtain / Build	Resolving the incident which would occur in the development environment
Deliver & Support	Identifying and resolving the incidents

Service Request Management

support the agreed quality of the service by handling the pre-defined user requests, which are initiated by users in a professional and friendly manner

SERVICE REQUEST MANAGEMENT

Service Request

a request from a user or a user's authorized representative initiates a service action that has been agreed as a regular part of service delivery

- Service Request are a normal part of service delivery

SERVICE REQUEST MANAGEMENT

Incidents vs Requests https://youtu.be/I6q7-oz1QdY

Service Request Catalog

a crucial part for the implementation of the process is the definition of the requests for an accurate planning of the supply processes for each type of request (Service Request Catalog)

SERVICE REQUEST MANAGEMENT

Use **automation** to the greatest degree possible

Seek out **opportunities** for improvement

Create **appropriate** policies to limit, remove, and minimize the need for additional approvals

Redirect incidents and problems to the appropriate practices

Optimize then automate & Manage expectation

Leverage existing workflow models

SERVICE REQUEST MANAGEMENT

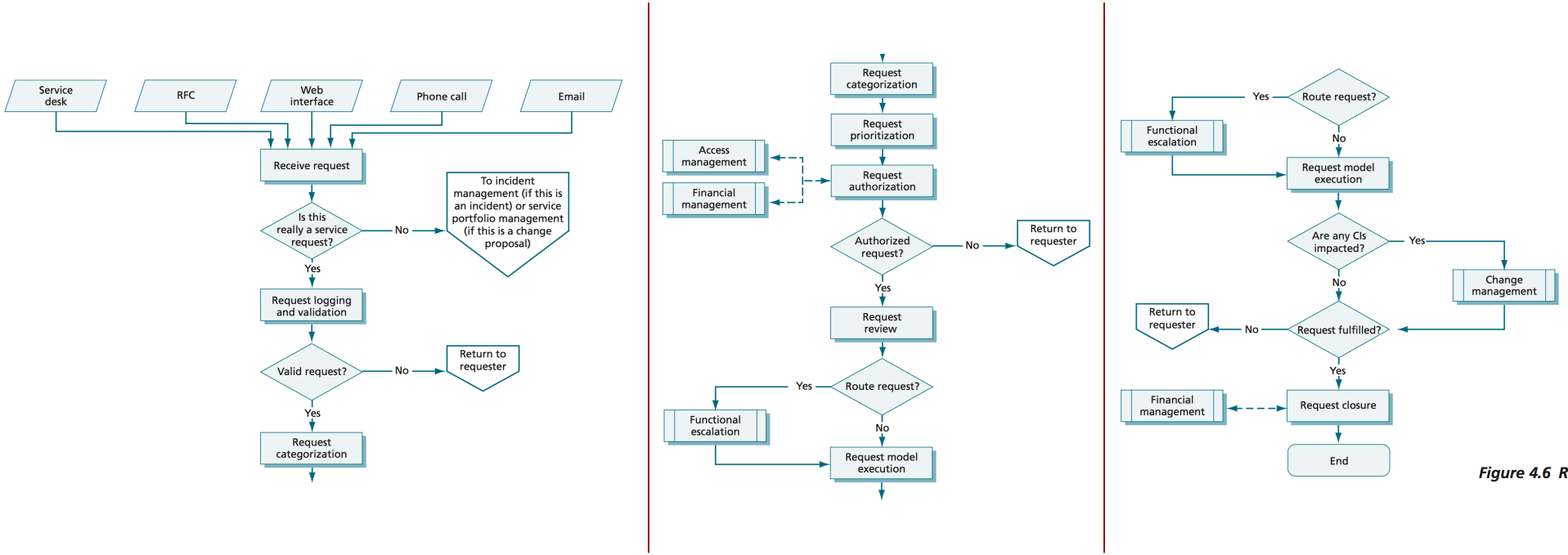
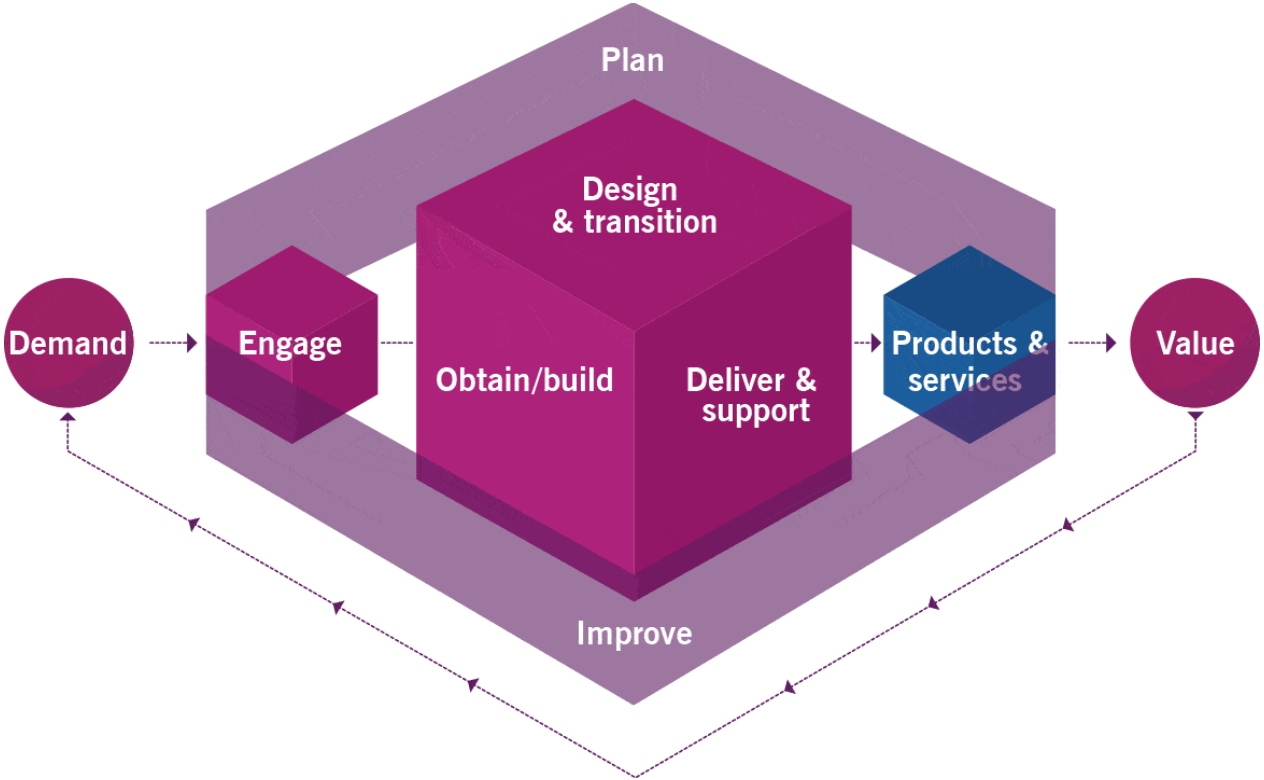


Figure 4.6 R

SERVICE REQUEST MANAGEMENT

Service Request Fulfillment – Explained using Pizza and online shopping
https://www.youtube.com/watch?v=LovnRgbaMY8

SERVICE VALUE CHAIN



SERVICE REQUEST MANAGEMENT

Plan	Uninvolved
Improve	Provide users a channel for improvement initiatives, compliments, and complaints
Engage	Provides regular communications to help set expectations
Design & Transition	Standard changes are used to initiate and fulfill service requests
Obtain / Build	Acquiring the services components required for fulfillment of service requests
Deliver & Support	Service request management makes a significant contribution to normal service delivery

SERVICE REQUEST MANAGEMENT | EXERCISE

- Create a template for a Service Request, what needs to be included in the template?

Problem Management

to identify the potential & actual causes of incidents and reduce the probability of the impacts of incidents by providing the solutions and workarounds, including the creation of known errors

Incidents vs Problems

we will go into more detail on this soon

PROBLEM MANAGEMENT

Problem	A cause, of one or more incidents
Known Error	A problem that has been analyzed and has not been resolved
Workaround	A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available
	Workarounds can be created at any stage

PROBLEM MANAGEMENT

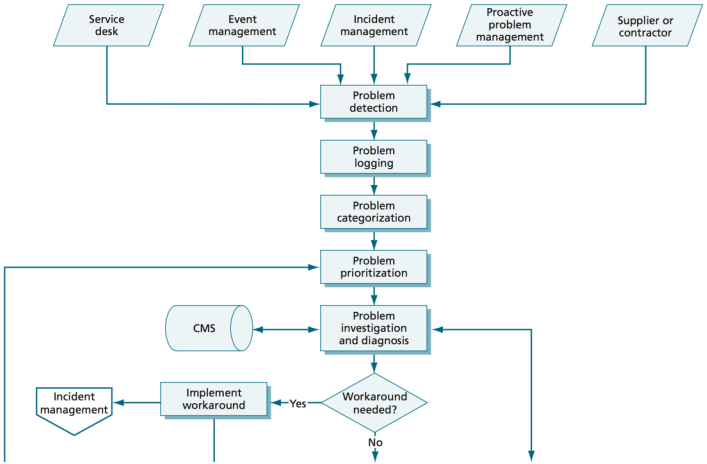
Problem Management involves three distinct phases, as shown in figure

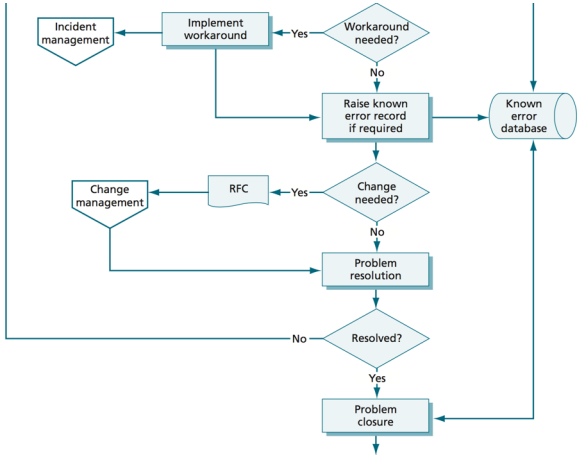
Problems are prioritized for analysis based on the risk that they pose, and are managed as risks based on their potential impact and probability

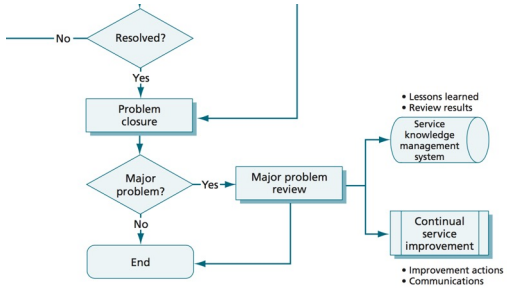
The responsibilities of this practice can be summarized as follows (subprocesses):

PROBLEM MANAGEMENT

PROBLEM MANAGEMENT - Explained using Doctor and Patient
https://www.youtube.com/watch?v=w1aOeF6P8kA


Service desk
Event management
Incident management
Proactive problem management
Supplier or contractor
Problem detection
Problem logging
Problem categorization
Problem prioritization
CMS
Problem investigation and diagnosis
Incident management
Implement workaround
Yes
Workaround needed?
No

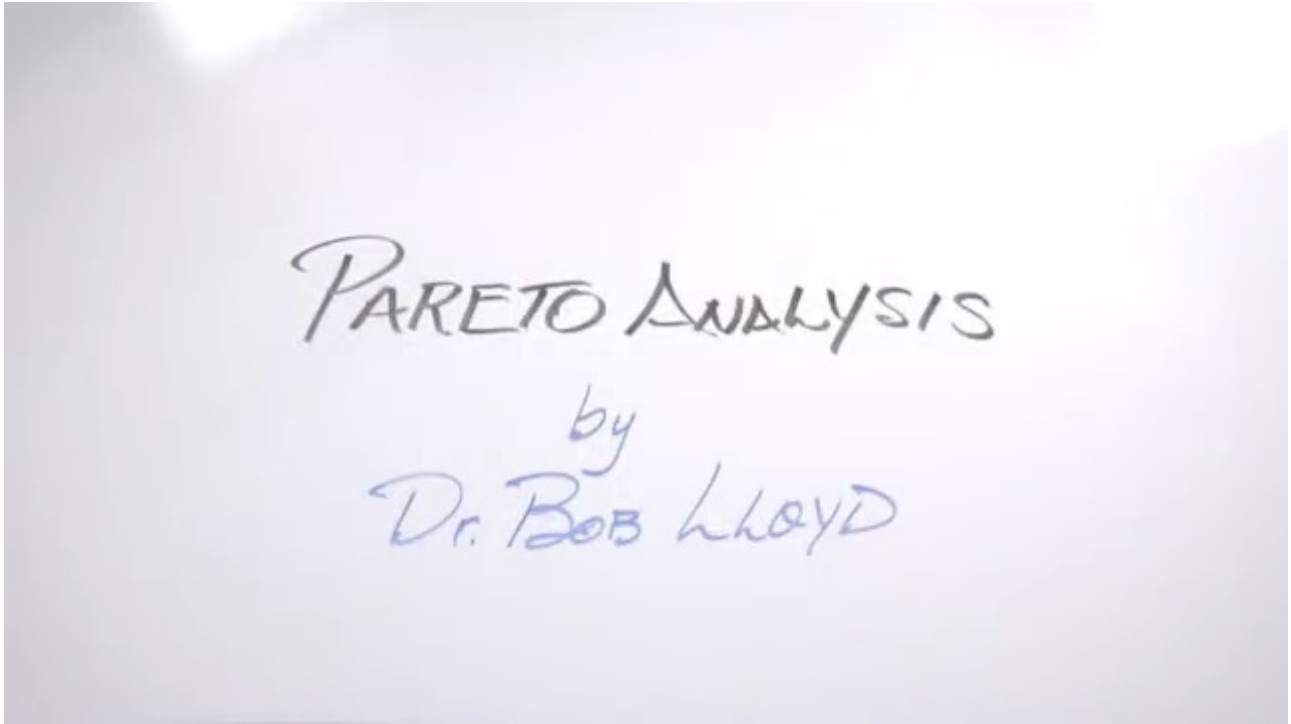

Incident management
Implement workaround
Yes
Workaround needed?
No
Raise known error record if required
Known error database
Change management
RFC
Yes
Change needed?
No
Problem resolution
No
Resolved?
Yes
Problem closure


No
Resolved?
Yes
Problem closure
Major problem?
Yes
Major problem review
No
End
• Lessons learned
• Review results
Service knowledge management system
Continual service improvement
• Improvement actions
• Communications

Problem Analysis Techniques

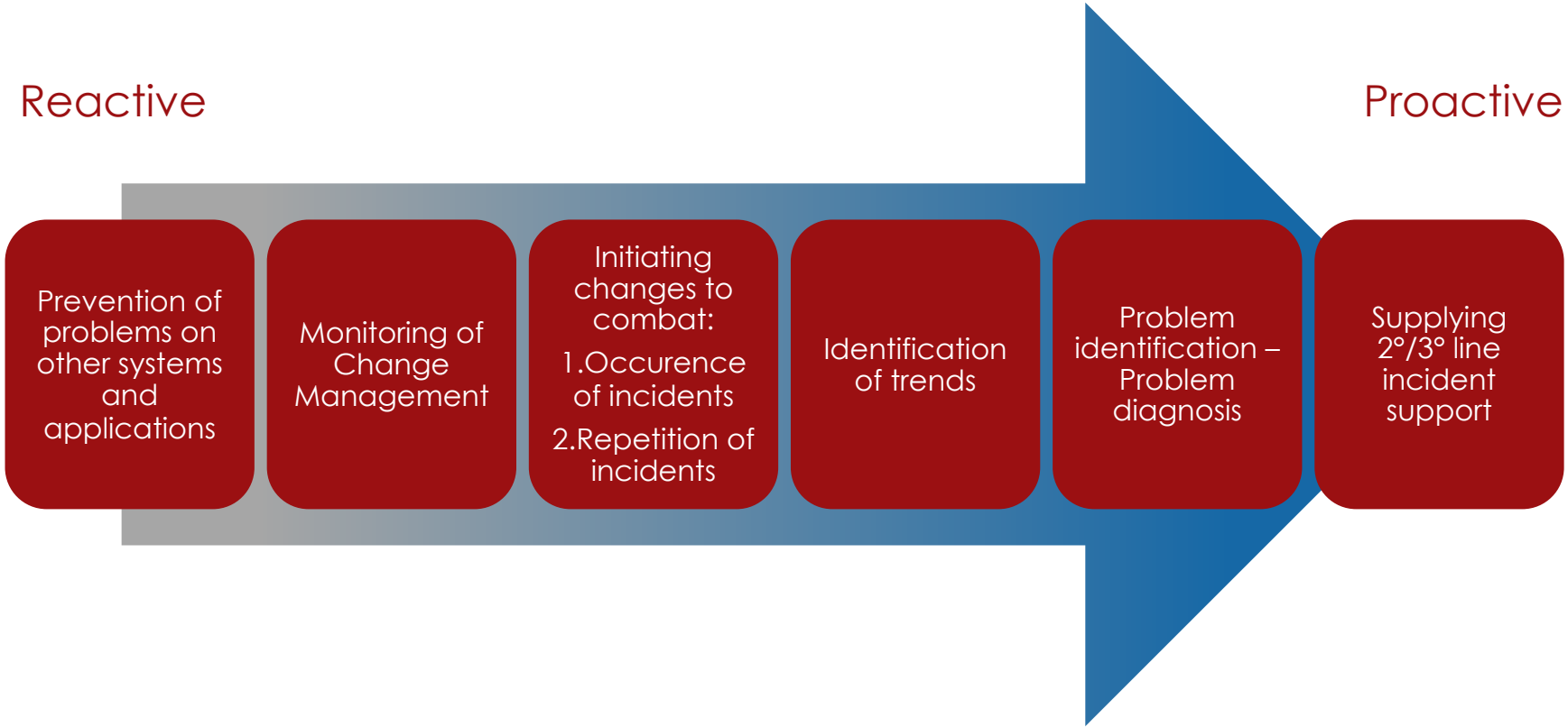
Problem situation	Suggested analysis techniques
Complex problems where a sequence of events needs to be assembled to determine exactly what happened	Chronological analysis Technical observation post
Uncertainty over which problems should be addressed first	Pain value analysis Brainstorming
Uncertain whether a presented root cause is truly the root cause	5-Whys Hypothesis testing
Intermittent problems that appear to come and go and cannot be recreated or repeated in a test environment	Technical observation post Kepner–Tregoe Hypothesis testing Brainstorming
Uncertainty over where to start for problems that appear to have multiple causes	Pareto analysis Kepner–Tregoe Ishikawa diagrams Brainstorming
Struggling to identify the exact point of failure for a problem	Fault isolation Ishikawa diagrams Kepner–Tregoe Affinity mapping Brainstorming
Uncertain where to start when trying to find root cause	5-Whys Kepner–Tregoe Brainstorming Affinity mapping

PROBLEM MANAGEMENT



Whiteboard: Pareto Analysis https://youtu.be/zbDRH2ASyqQ

PROBLEM MANAGEMENT



PROBLEM MANAGEMENT

The "Proactive Control Management" sub-process carries out those activities aimed at identifying and resolving problems before they can cause incidents.

These activities are:

- Trend Analysis
- Targeting Support Action
- Informing the organization

By redirecting the efforts of an organization from reactive towards a large number of preventative incidents, an organization provides a better service to its customers and makes the use of available resources within the IT support organization more effective and efficient.

Trend Analysis

Incident and problem reporting can provide information for preventive measures to improve service quality

Incident and problem analyzes can identify trends such as:

- The occurrence of a certain type of problem as a result of a change
- The beginning of a certain type of anomaly or malfunction
- The repetition of particular incidents and problems with some CIs in particular
- The need to train the staff or the customer

Targeting Support Action

Trend Analysis can lead to the identification of faulty parts in the IT infrastructure, which can then be analyzed and corrected

It can also lead to the identification of problem areas that need more attention from the support

Informing the organization

Problem Management can provide information about problems, KEs and RFCs issued

This helps to determine the health of the business and the details can be used to inform the "decision making" processes within the organization and other practices such as Service Level Management and Service Desk

PROBLEM MANAGEMENT

Proactive and Reactive Problem Management
https://youtu.be/LOgGTdERCLM

The benefits of a formal approach to Problem Management include:

- Improvement of the quality of IT service
  The PM helps to create a cycle of rapid increase in the quality of IT service, and is good for the productivity and mood of those who provide the IT service

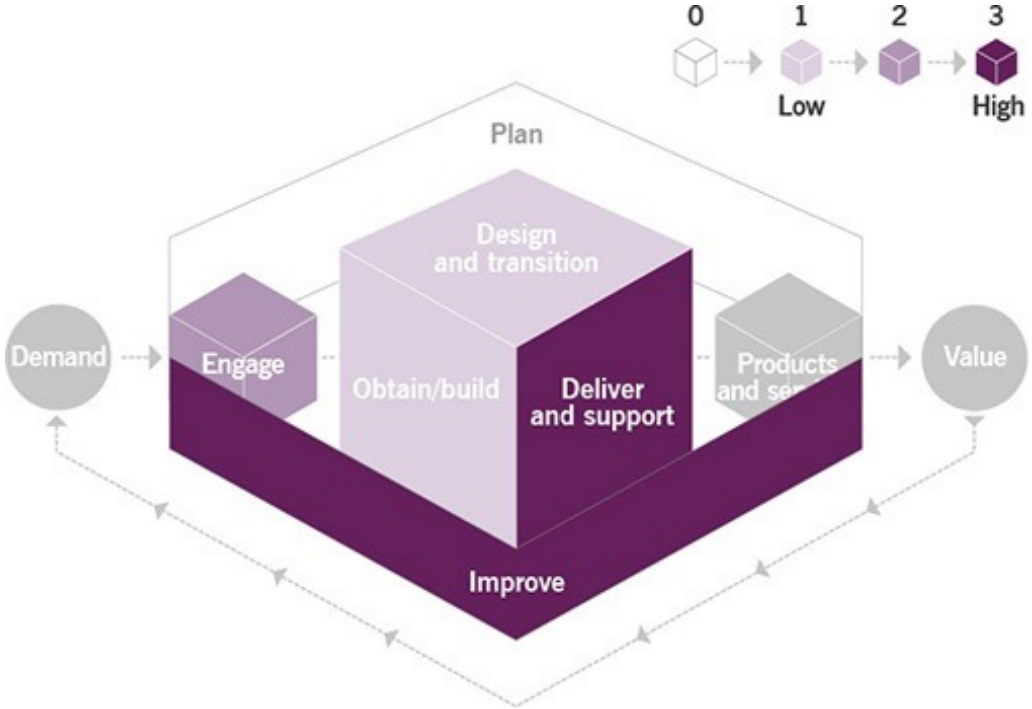
- Reduction in the volume of accidents
  PM contributes to reducing the number of incidents that disrupt the conduct of business

- Permanent solutions
  There is a gradual reduction in the number and impact of Problems and KEs once those solved remain solved

- Improvement of the level of learning at the organizational level.
  The PM process is based on the concept of learning from past experiences. The process provides historical data to allow the identification of trends, a means of preventing failures and reducing the impact of these, resulting in improved user productivity

- Greater number of fixes working since the first time available to the SD.
  The PM provides the SD with more incident fixes that work on the first try thanks to the information-based process of the CMDB

PROBLEM MANAGEMENT



Heat map of the contribution of problem management to value chain activities

PROBLEM MANAGEMENT

Plan	Uninvolved
Improve	Provides an understanding of how to reduce incidents and their impact
Engage	Involving the required stakeholders for problem prioritization and resolution
Design & Transition	Providing the information that will help in improved testing and knowledge transferring
Obtain / Build	Managing the product defects identified by problem management
Deliver & Support	Preventing recurrence of incidents and supporting timely incident resolution

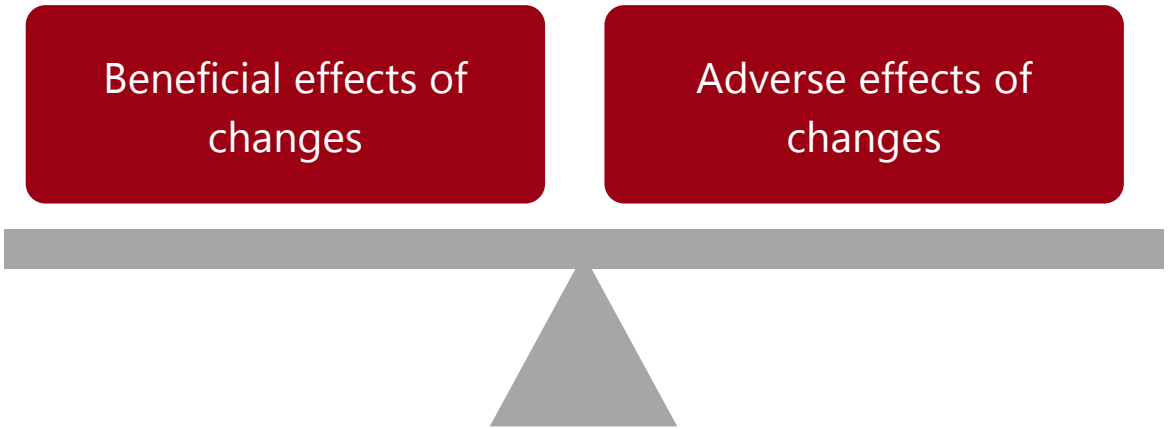
Change Enablement

maximize the number of successful service and product changes by ensuring that risks have been properly assessed, authorizing changes to proceed, and managing the change schedule

- Business today requires a highly controlled IT environment
- The first goal is to ensure that standardized methods and procedures are in place to make changes: balancing between the need for a change and its impact
- No bureaucracy but reduce the need to make continuous ad hoc changes.
- Managing change has become a full-time job

Change Enablement

must balance the need to make beneficial changes that will deliver additional value with the need to protect customers and users from the adverse effect of changes



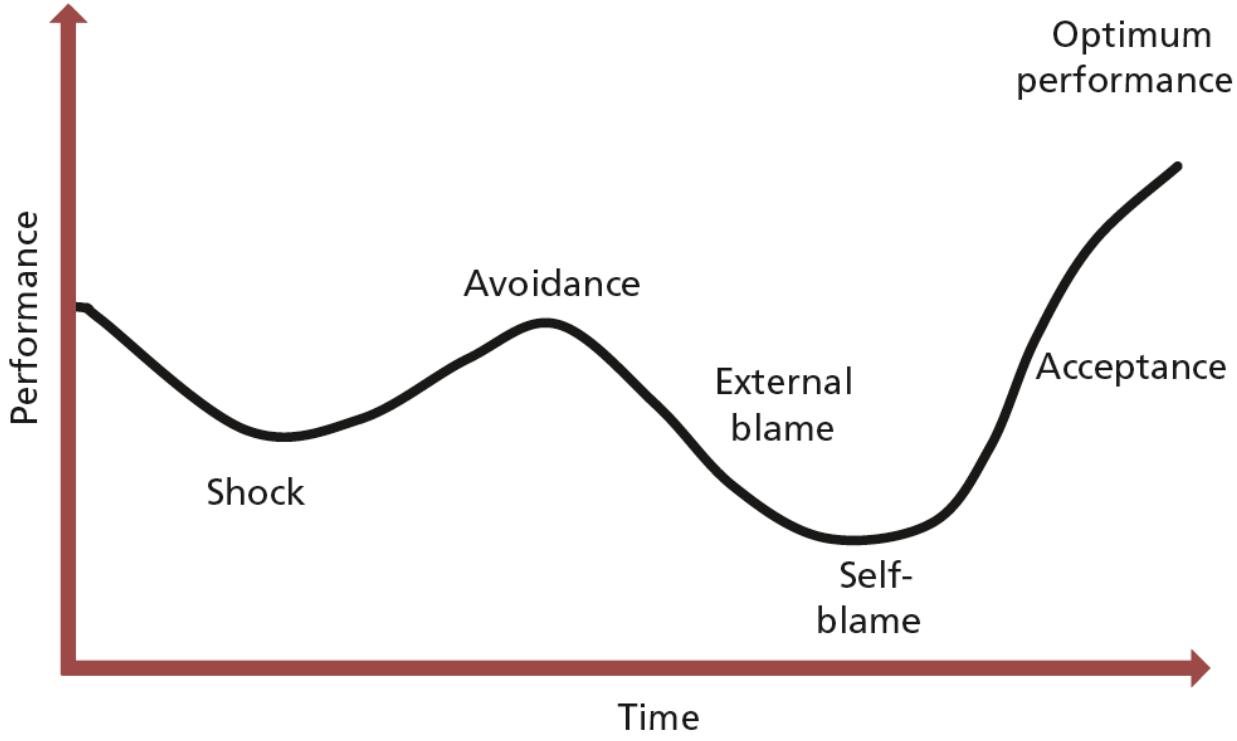
Change

the addition, modification, or removal of anything that could have a direct or indirect effect on services

THE 7 R OF CHANGE MANAGEMENT

- Who Raised the Change?
- What is the Reason for the Change?
- What is the Return required from the Change?
- What are the Risks involved in the Change?
- What Resources are required to deliver the Change?
- Who is Responsible for the build, test and implementation of the Change?
- What is the Relationship between this Change and other Changes?

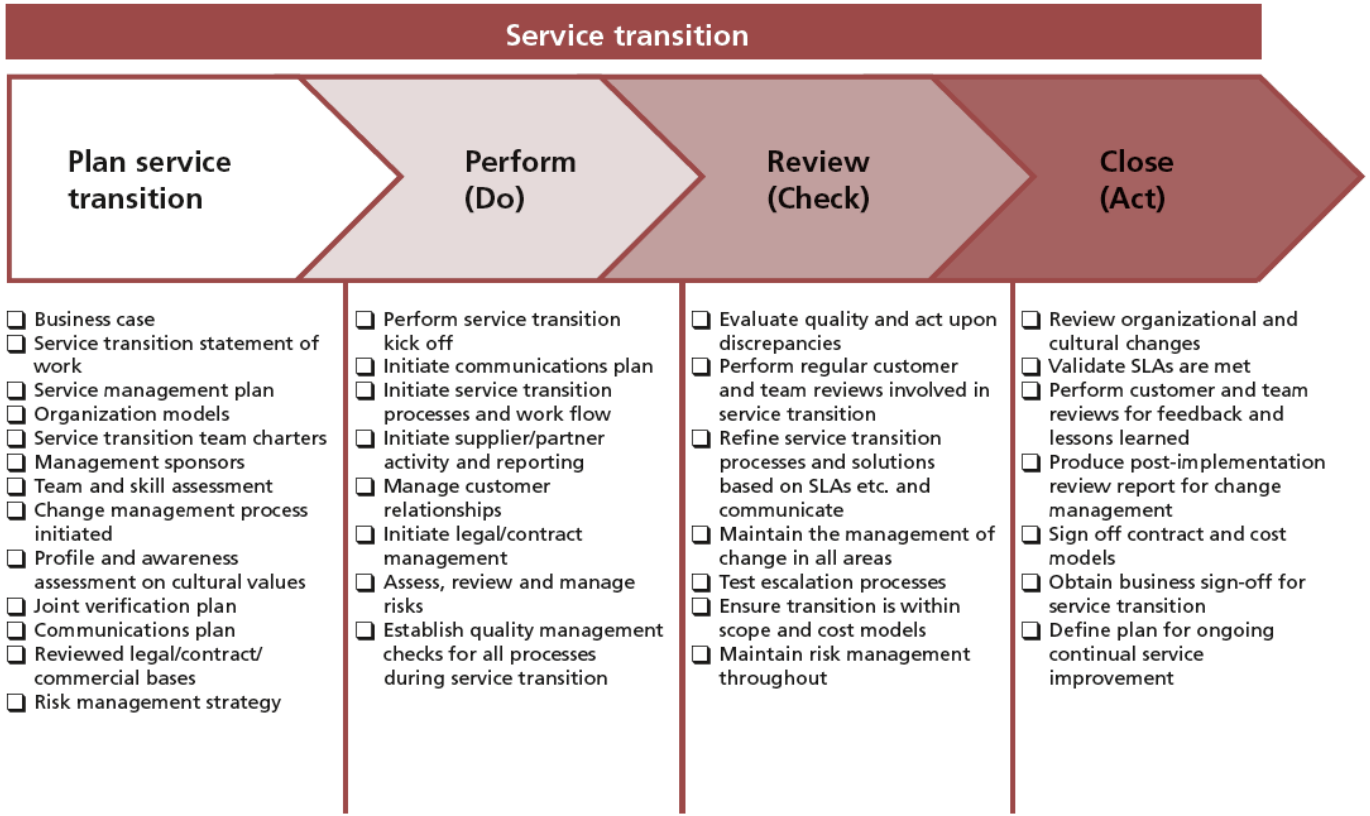
THE EMOTIONAL CYCLE OF CHANGE



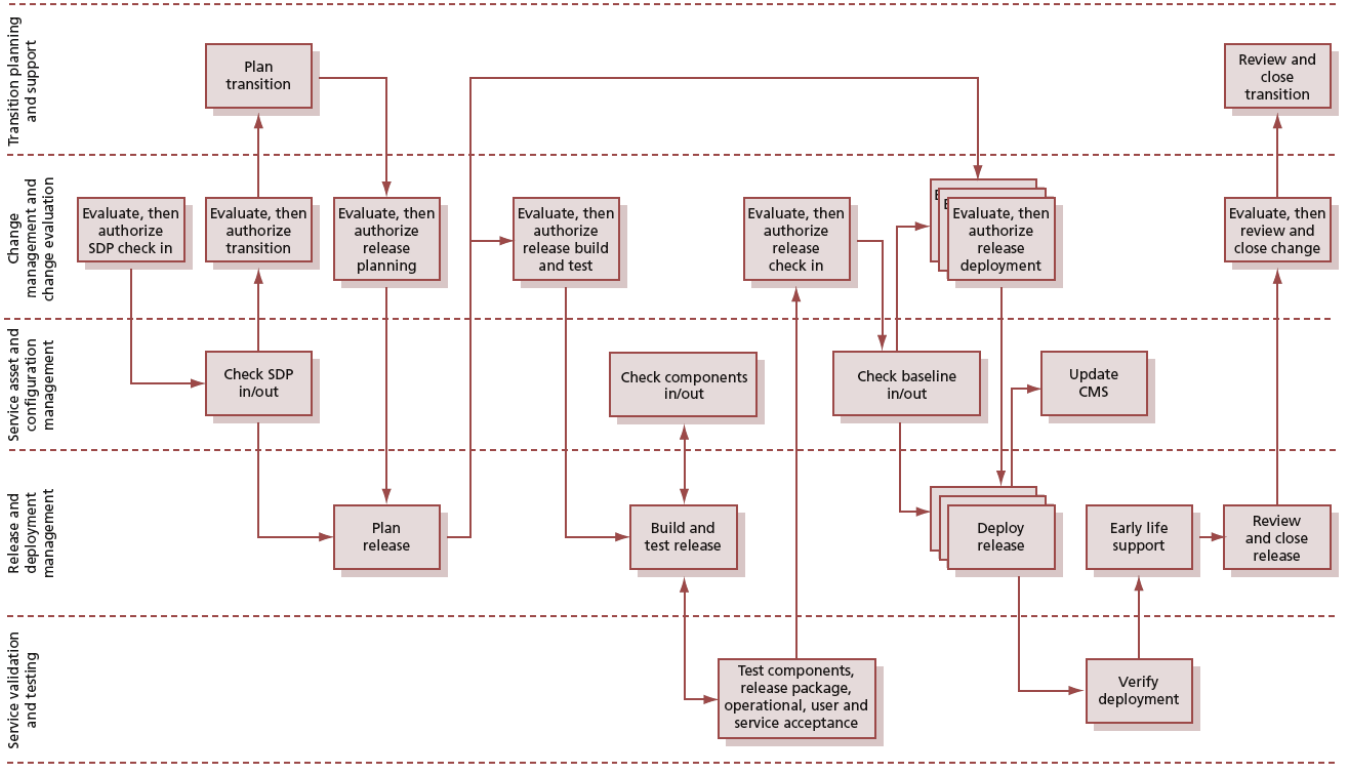
CHANGE RACI MATRIX

Role responsibility	Change sponsor, e.g. business and IT leader	Change enabler, e.g. process owner, service owner	Change agent, e.g. team leader instructing change	Change target, e.g. individual performing the change
Articulate a vision for the business and service change in the domain	AR	R	C	I
Recognize and handle resistance to change	R	A	R	C
Initiate change, understand the levers for change and the obstacles	R	AR	C	C
Manage change and input to change plan	C	AR	C	C
Input to design of target organization or structure, etc.	C	AR	C	I
Set up a system for communicating change	AR	R	C	I
Steer change	AR	R	R	C
Mobilize the organization	AR	C	C	C
Mobilize the department, unit, team	AR	R	R	I
Lead workshops and group analysis of the current processes	I	AR	R	I

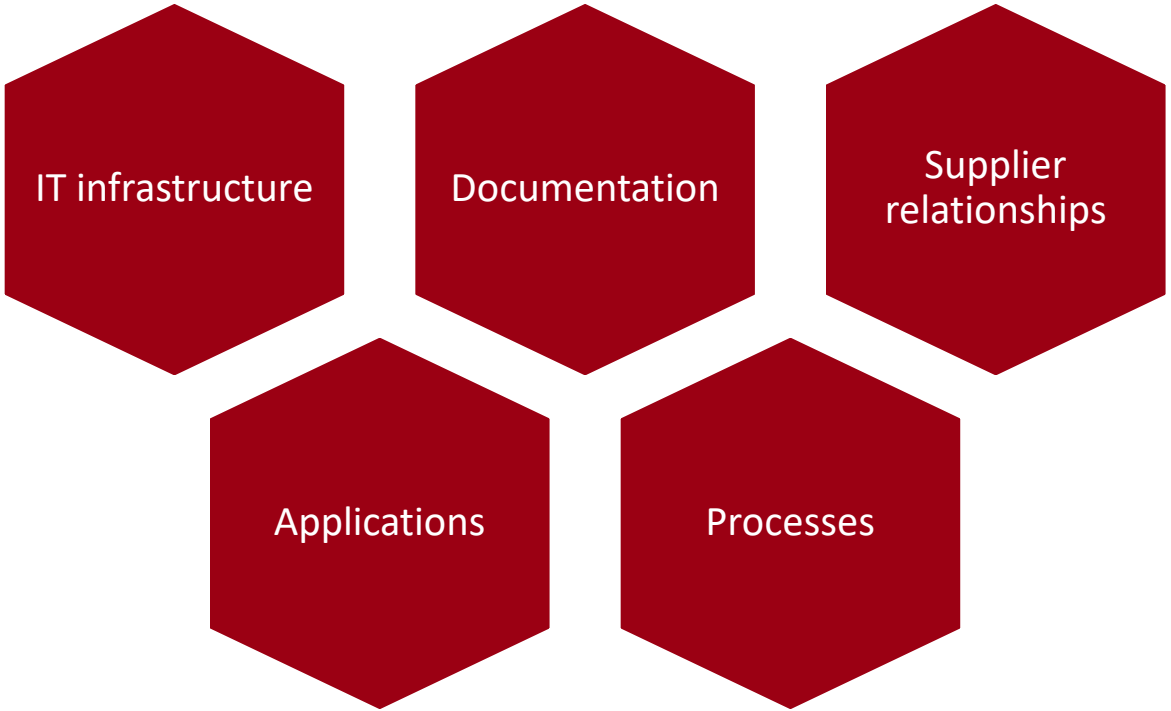
Service Transition In OutSourcing



EXAMPLE OF A PATH THROUGH THE PROCESSES



CHANGE ENABLEMENT



Change Priority

Priority	Corrective change	Enhancement change
Immediate Treat as emergency change (see section 4.2.5.11)	Putting life at risk Causing significant loss of revenue or the inability to deliver important public services Immediate action required	Not appropriate for enhancement changes
High To be given highest priority for change building, testing and implementation resources	Severely affecting some key users, or impacting on a large number of users	Meets legislative requirements Responds to short-term market opportunities or public requirements Supports new business initiatives that will increase company market position
Medium	No severe impact, but rectification cannot be deferred until the next scheduled release or upgrade	Maintains business viability Supports planned business initiatives
Low	A change is justified and necessary but can wait until the next scheduled release or upgrade	Improvements in usability of a service Adds new facilities

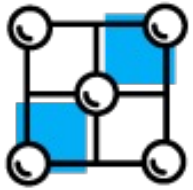
CHANGE ENABLEMENT

STANDARD

- Straightforward
- Frequent
- Documentation needed
- No authorization by CAB needed

NORMAL

- Important
- Full review
- Requires CAB authorization



MAJOR

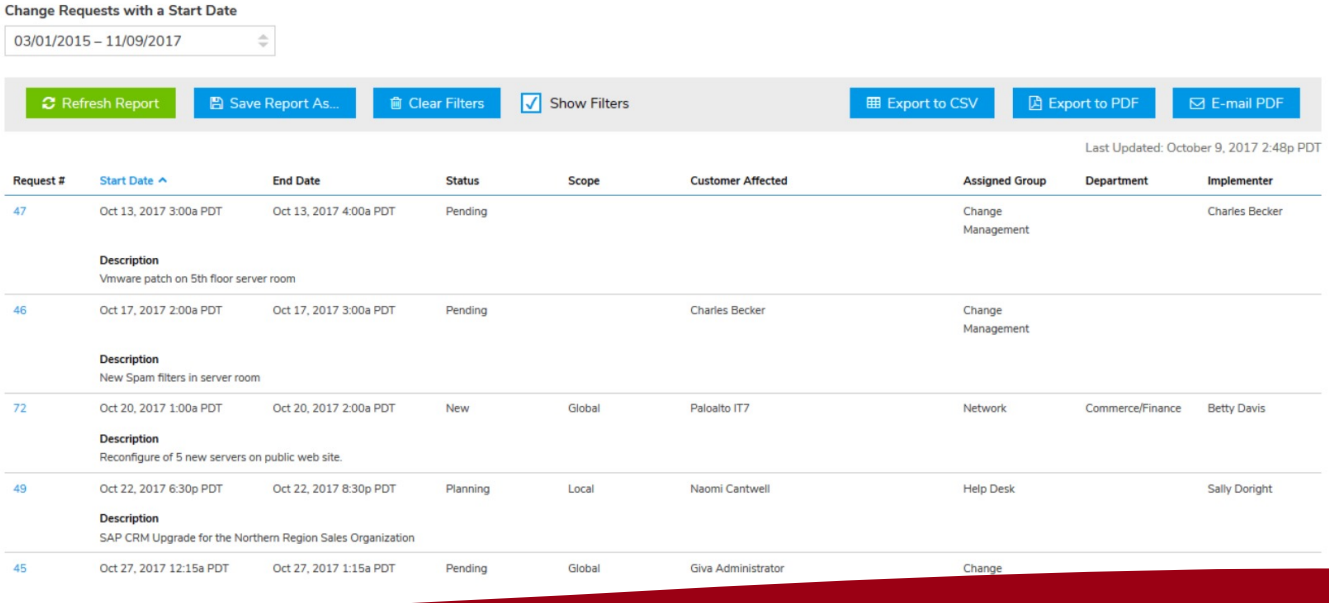
- High risk
- Detailed report
- Requires CAB & management authorization

EMERGENCY

- Urgent
- Resolves incident
- High risk of failure
- Flexible pool of approvers

Change Schedule (CS)

(formerly the ITIL v2 Forward Schedule of Change (FSC)) contains the details of all the changes authorized for implementation, accompanied by the expected dates



Change Requests with a Start Date

03/01/2015 – 11/09/2017

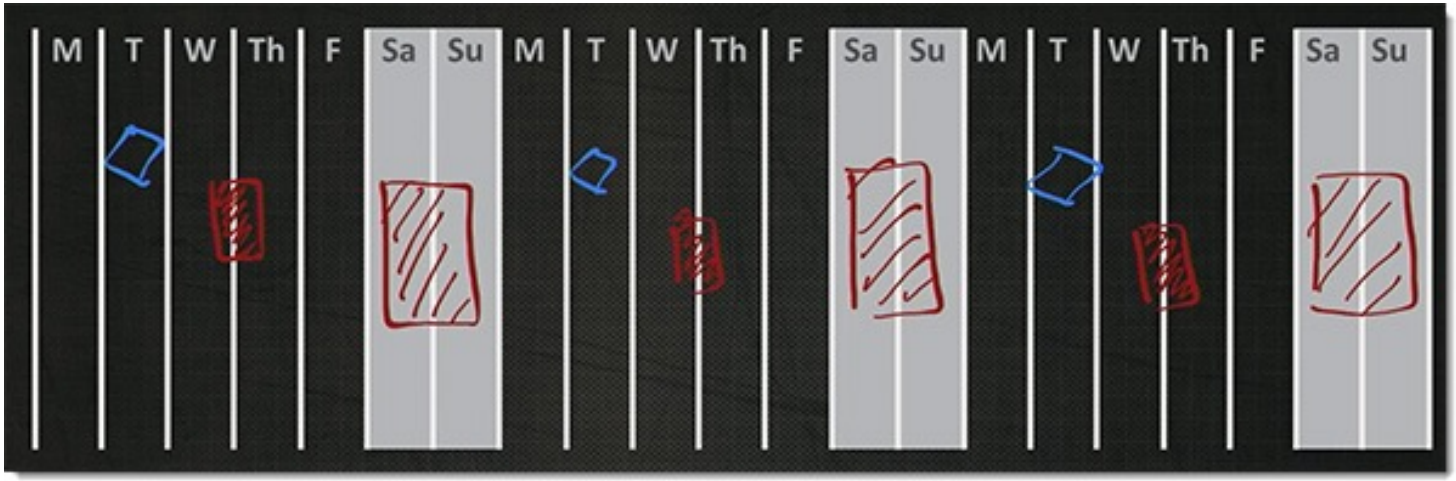
Refresh Report | Save Report As... | Clear Filters | Show Filters | Export to CSV | Export to PDF | E-mail PDF

Last Updated: October 9, 2017 2:48p PDT

Request #	Start Date	End Date	Status	Scope	Customer Affected	Assigned Group	Department	Implementer
47	Oct 13, 2017 3:00a PDT	Oct 13, 2017 4:00a PDT	Pending			Change Management		Charles Becker
	Description Vmware patch on 5th floor server room							
46	Oct 17, 2017 2:00a PDT	Oct 17, 2017 3:00a PDT	Pending		Charles Becker	Change Management		
	Description New Spam filters in server room							
72	Oct 20, 2017 1:00a PDT	Oct 20, 2017 2:00a PDT	New	Global	Paloalto IT7	Network	Commerce/Finance	Betty Davis
	Description Reconfigure of 5 new servers on public web site.							
49	Oct 22, 2017 6:30p PDT	Oct 22, 2017 8:30p PDT	Planning	Local	Naomi Cantwell	Help Desk		Sally Doright
	Description SAP CRM Upgrade for the Northern Region Sales Organization							
45	Oct 27, 2017 12:15a PDT	Oct 27, 2017 1:15a PDT	Pending	Global	Giva Administrator	Change		

Projected Service Outage (PSO)

contains the details of the changes according to the SLAs and the agreed maintenance windows, the planned downtime also for other reasons such as maintenance or data backup



CHANGE ENABLEMENT

ITIL - Change Management a Change Schedule for your Change Advisory Board (CAB)
https://youtu.be/q3vUVXOp6_U

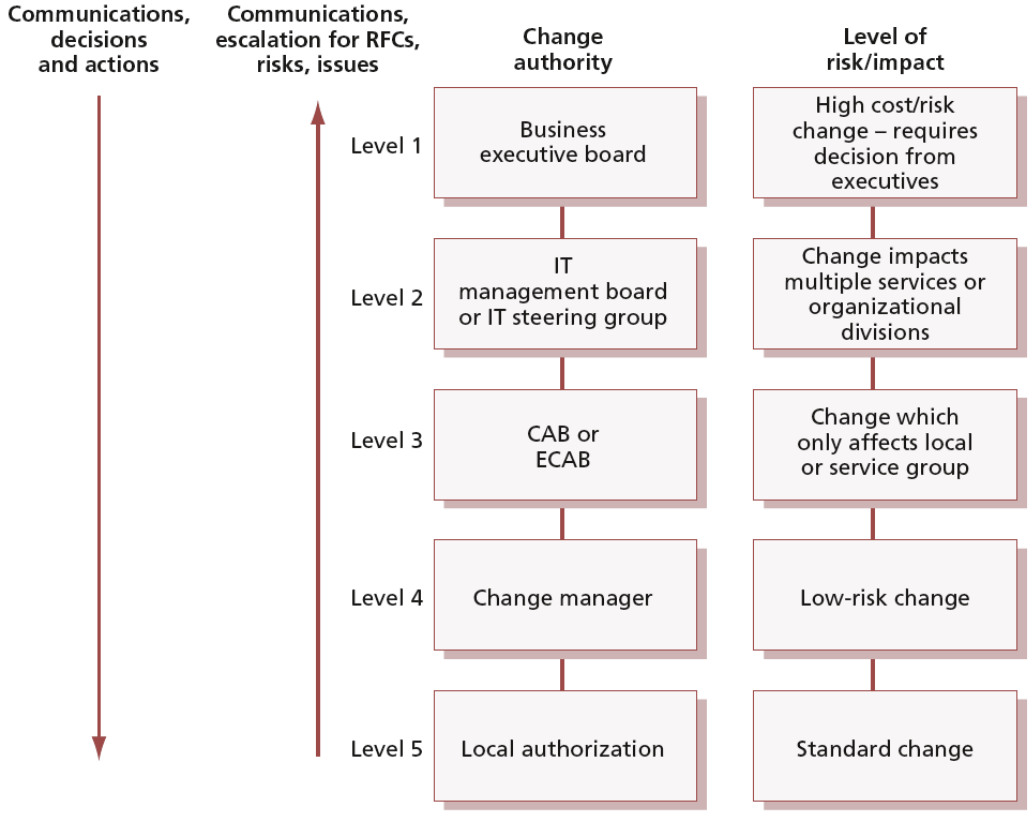
Change Authority

a person or group responsible for authorizing a change

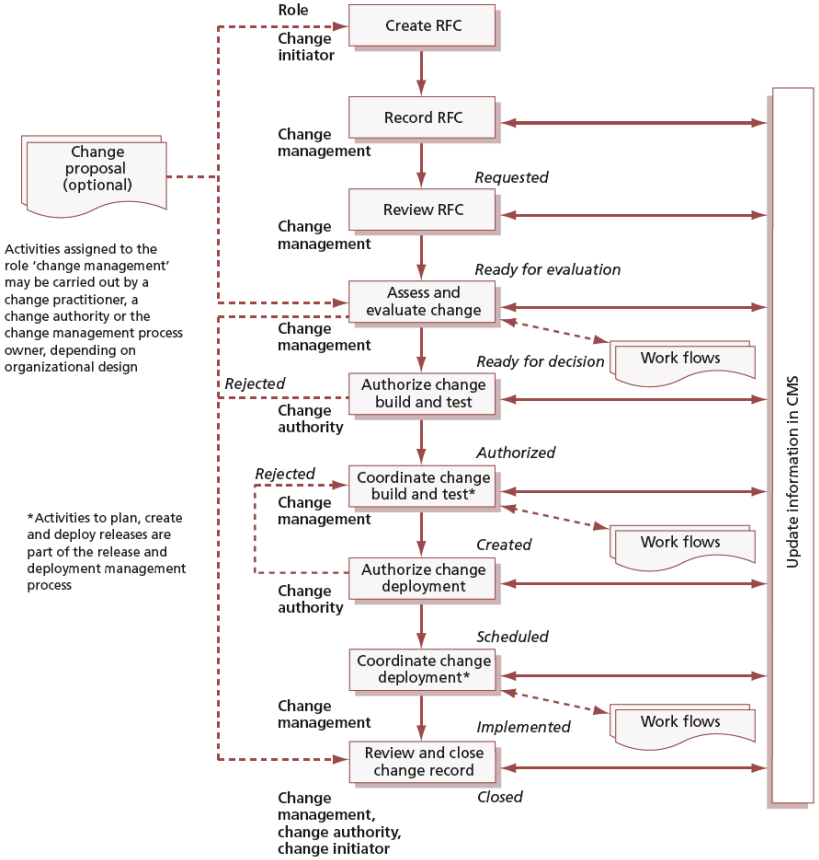
Change Advisory Board (CAB)

The CAB is not static but can change according to the level of risk to which the change is subject

On the right, an example of a change authorization model

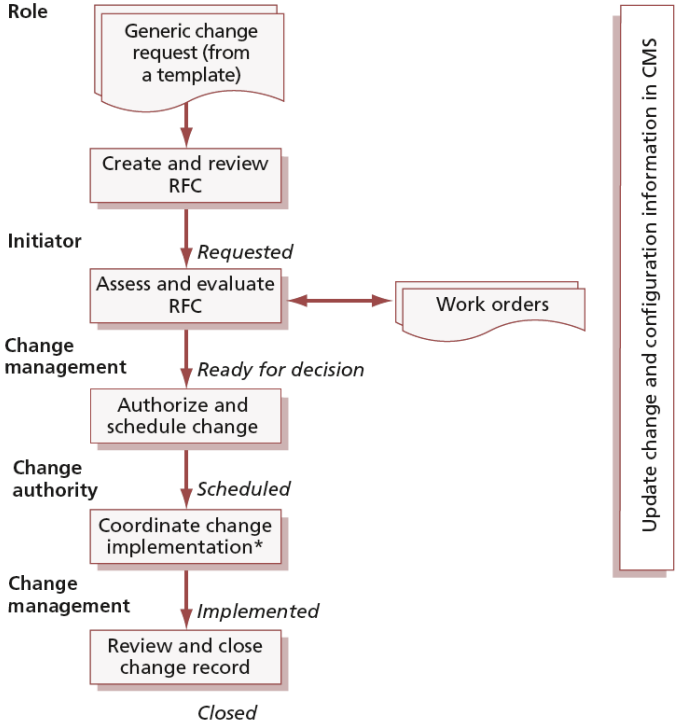


CHANGE ENABLEMENT



Typical flow for a Normal Change

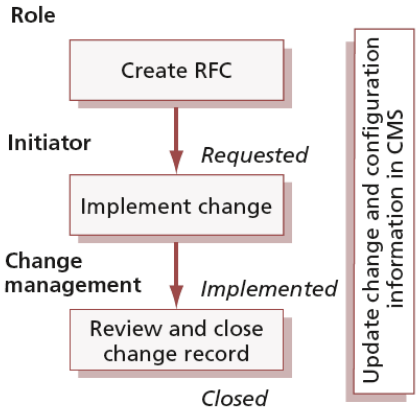
Standard deployment request (where the deployment process is tried and tested)



*Includes build and test the change

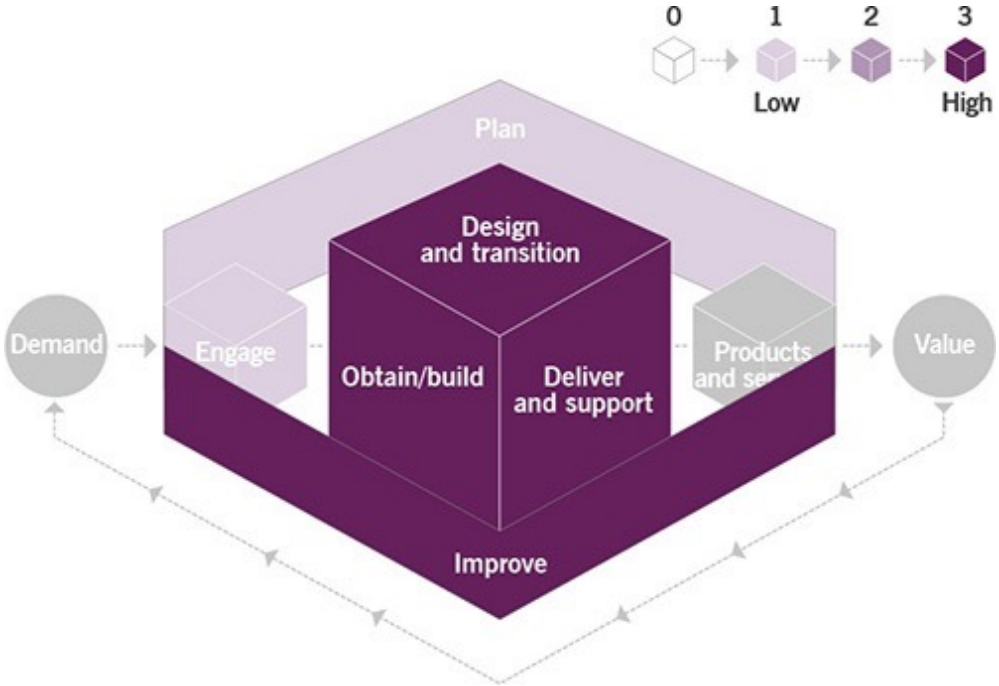
Typical flow for a Standard Deployment Request

CHANGE ENABLEMENT



Typical flow for a standard Operational Change Request

CHANGE ENABLEMENT

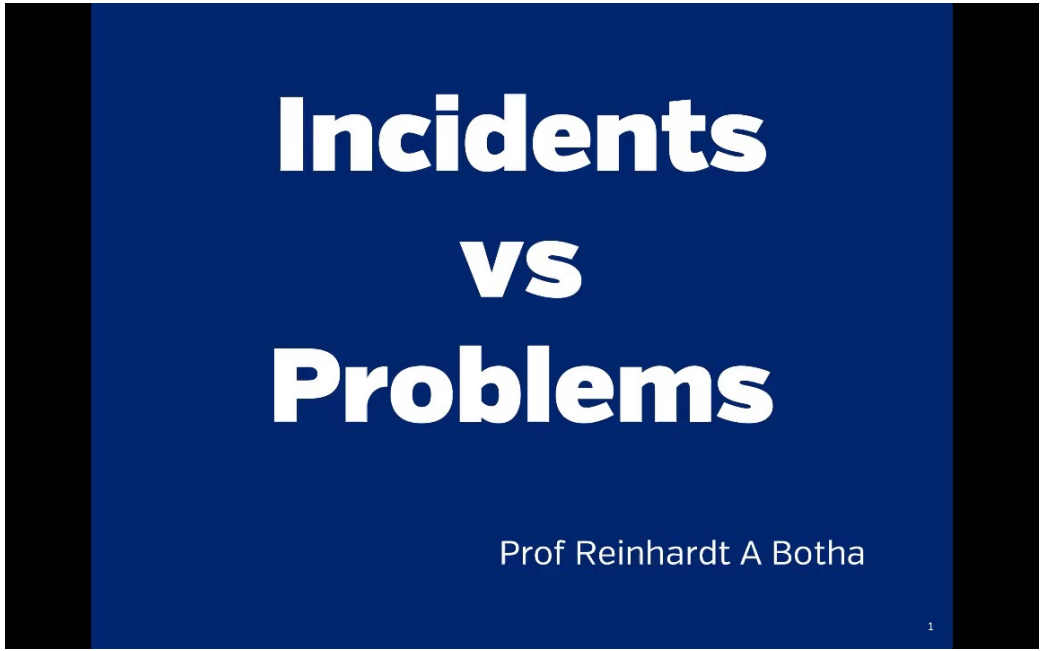


Heat map of the contribution of change enablement to value chain activities

CHANGE ENABLEMENT

Plan	Modeling the change control for changes to process, products, service portfolio etc. at all levels
Improve	Improvement of change control practices, i.e., the way change is being handled
Engage	Engaging with the stakeholders required for execution, informing, consulting etc. while doing the change
Design & Transition	Defining & transitioning the change
Obtain / Build	Acquiring & building the service components required for proposed change
Deliver & Support	Informing, coordinating, communicating, monitoring the changes & its impacts, before and after the execution of change

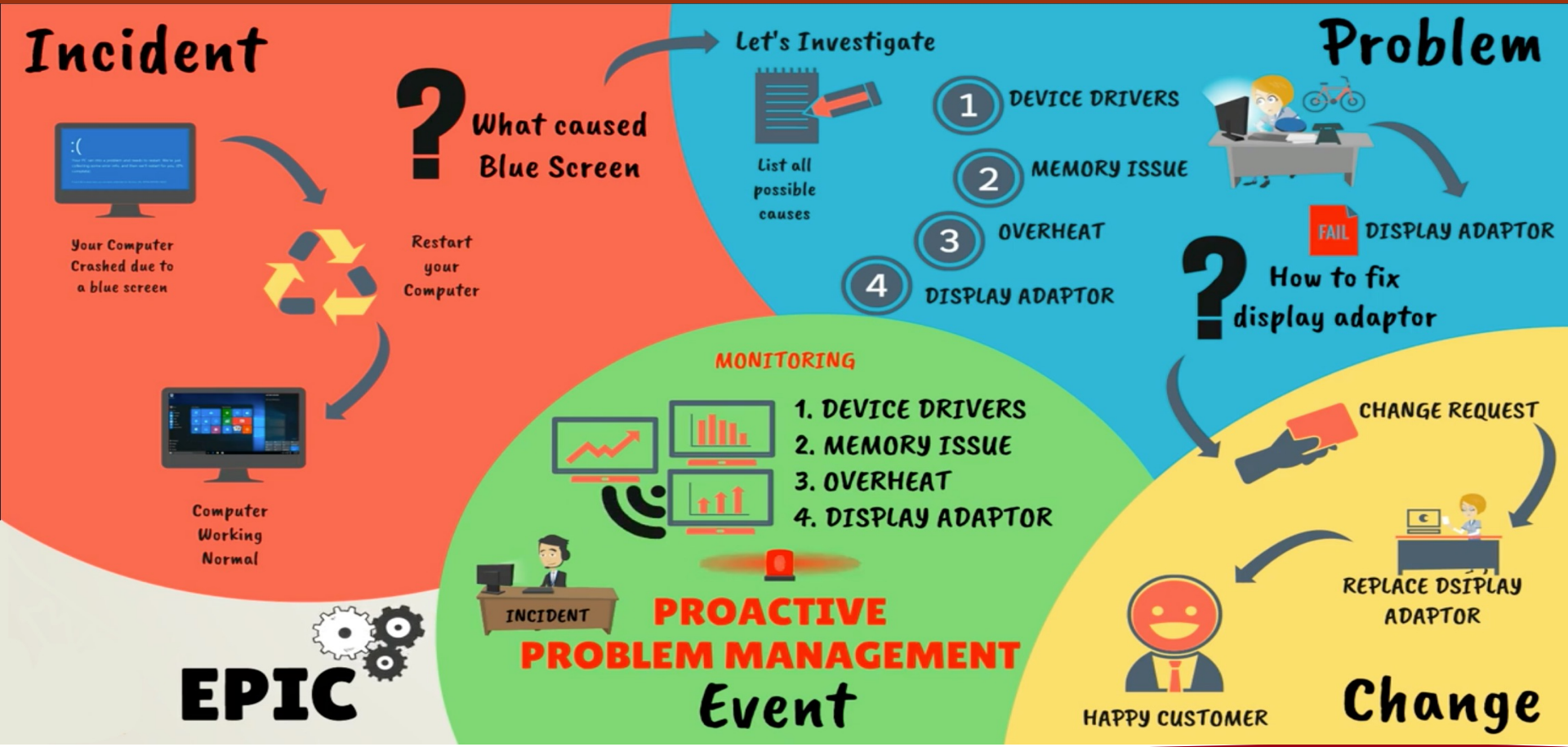
E vent
P roblem
I ncident
C hange

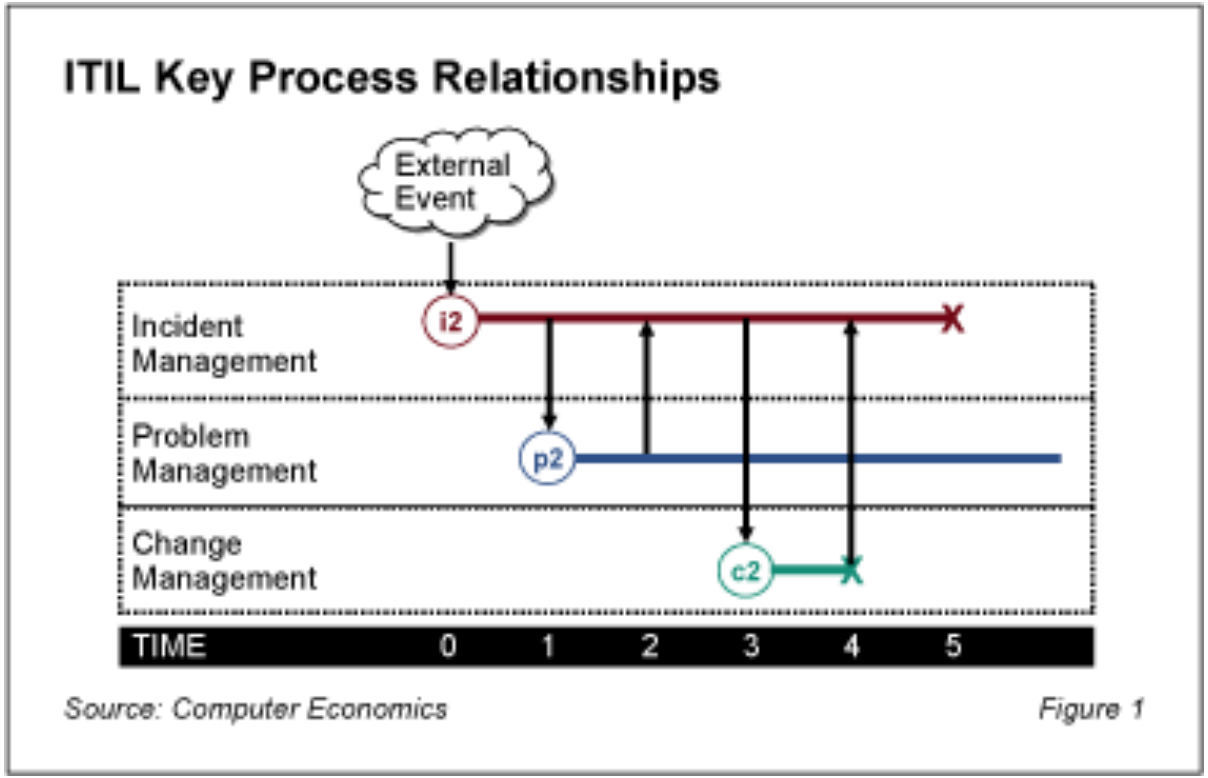


Incident vs Problems https://youtu.be/H759gbooew4

EPIC https://www.youtube.com/watch?v=NOznQoxo44I

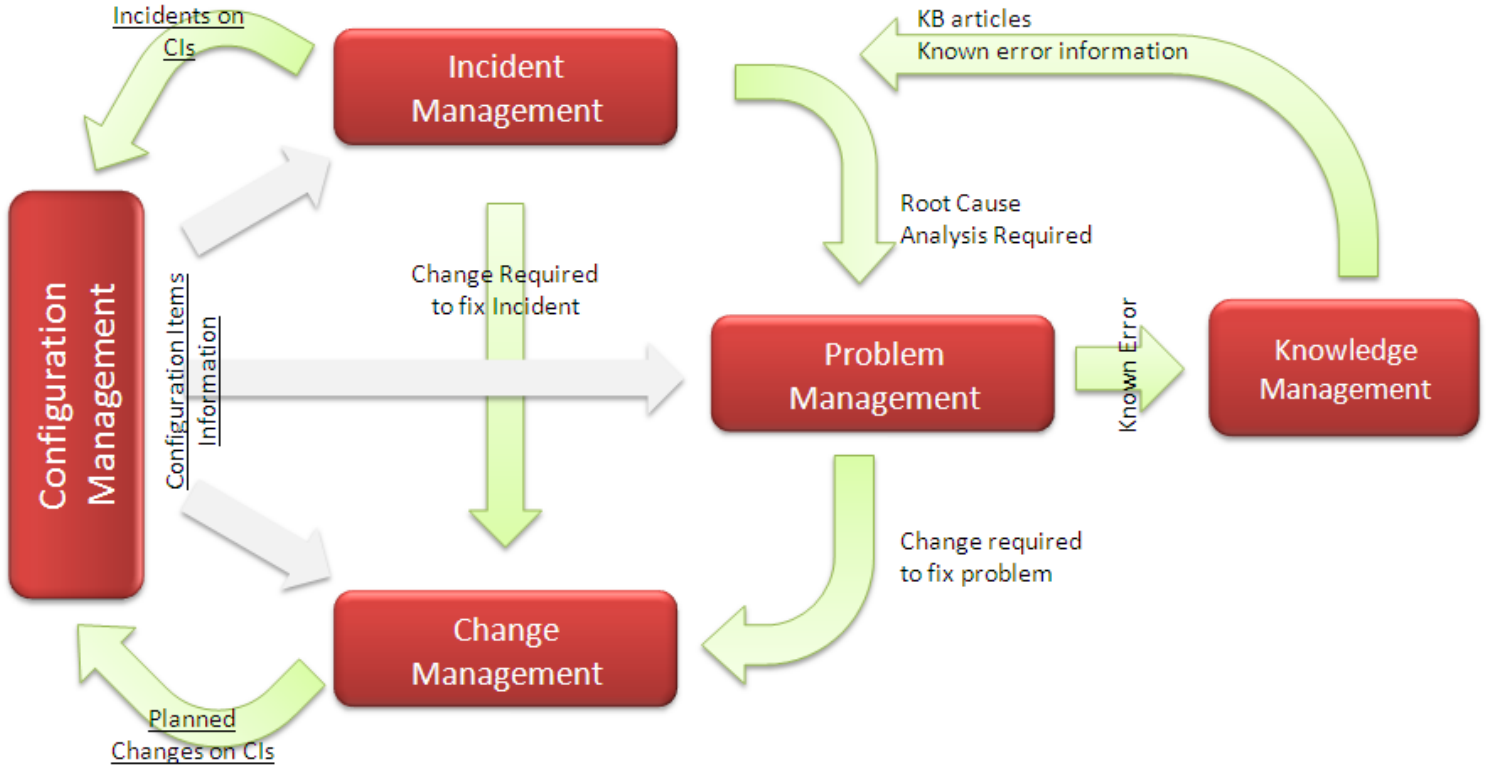
SERVICE MANAGEMENT PRACTICES



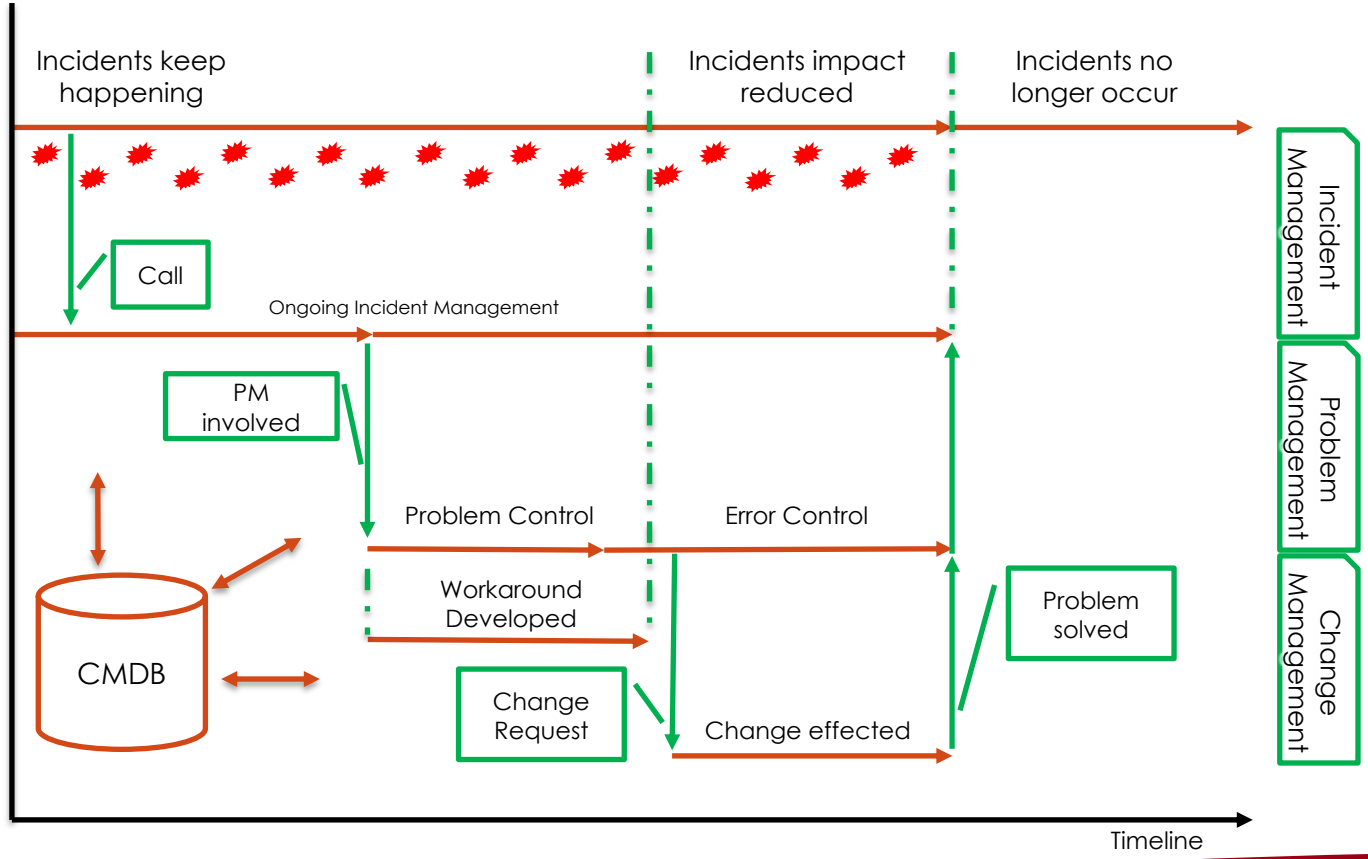


Source: Computer Economics

Figure 1

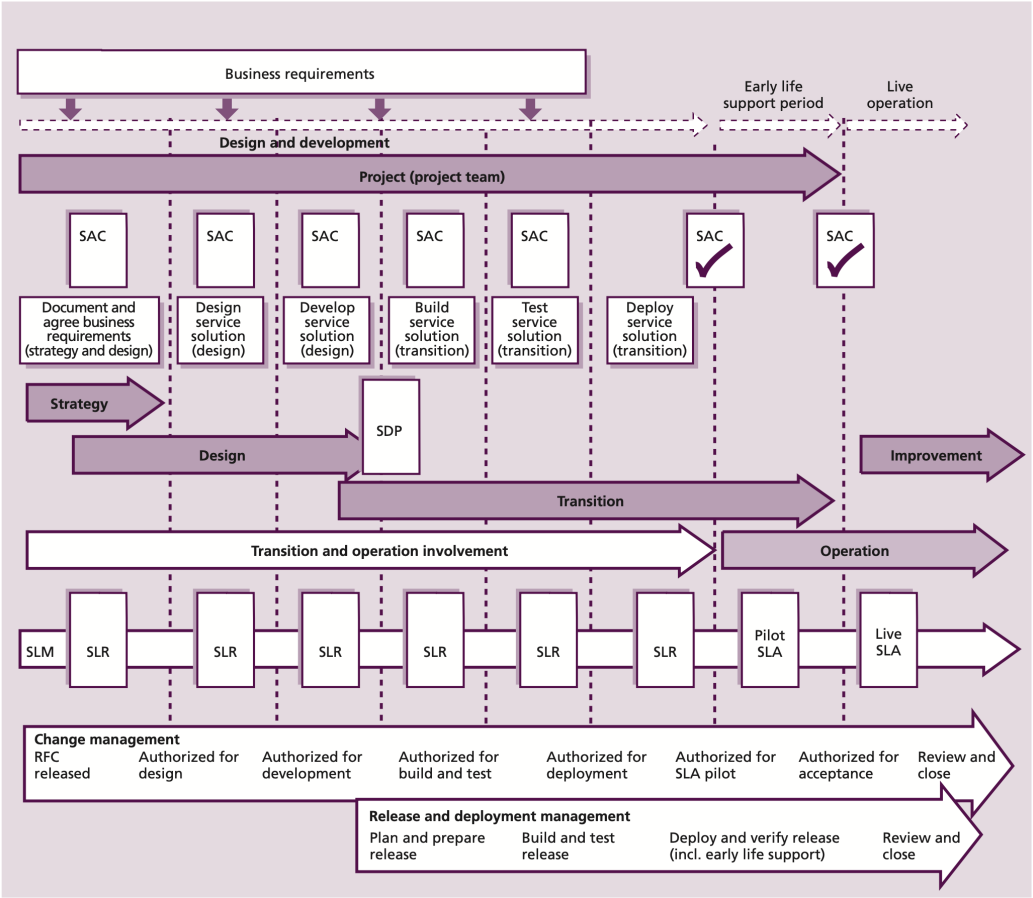

Incidents on CIs
Incident Management
KB articles
Known error information
Root Cause Analysis Required
Configuration Management
Configuration Items Information
Change Required to fix Incident
Problem Management
Known Error
Knowledge Management
Change required to fix problem
Change Management
Planned Changes on CIs

SERVICE MANAGEMENT PRACTICES



The figure shows the lifecycle of a service from the initial or changed business requirement through the design, transition and operation stages of the lifecycle.

It is important that there is effective transfer of knowledge at all stages between the operational staff and the project staff to ensure smooth progression through each of the stages illustrated.



Service Desk

capture demand for incident resolution and service requests

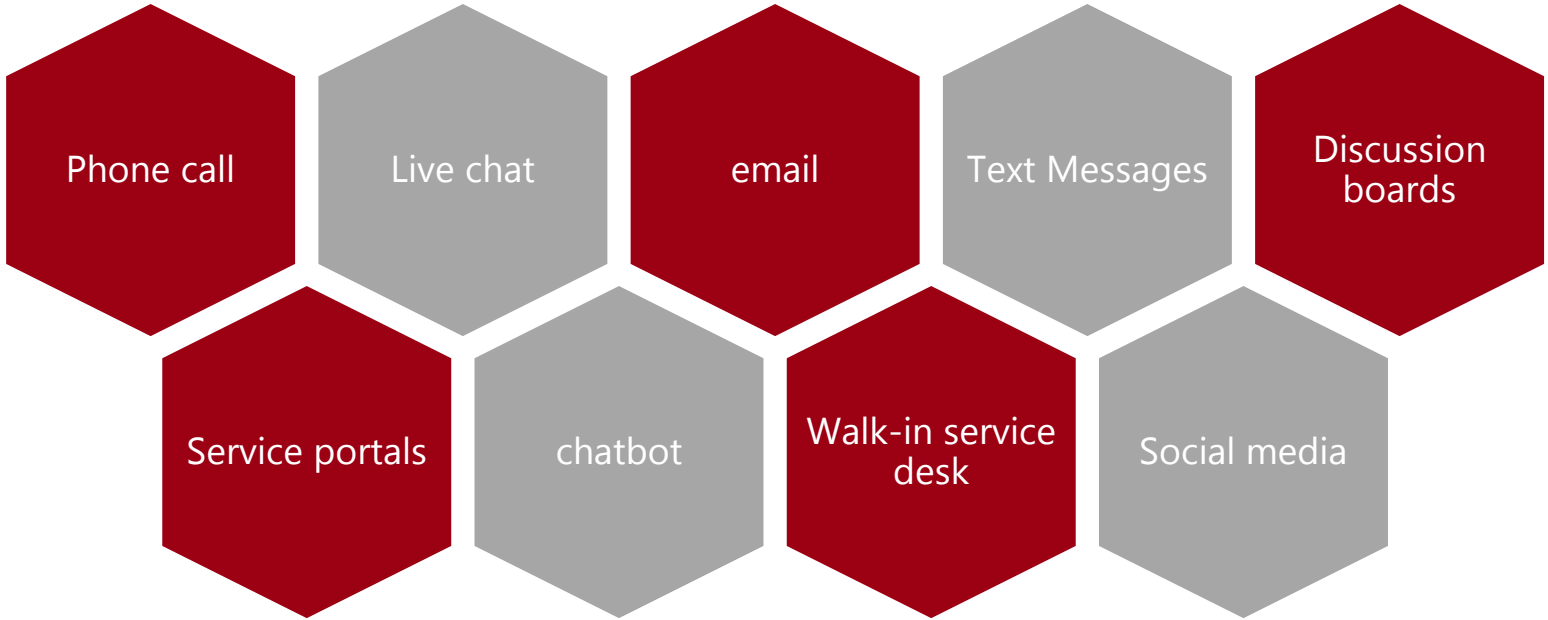
The purpose of the service desk practice is to:

- Understand demand for incident resolution and service requests
- Act as the point of contact for the service provider along with its users
- Provide a clear path for users to report issues, queries, and requests, and acknowledge, classify, own, and take action on them

SERVICE DESK

Key Aspects of Service Desk

Channels of Service Desk



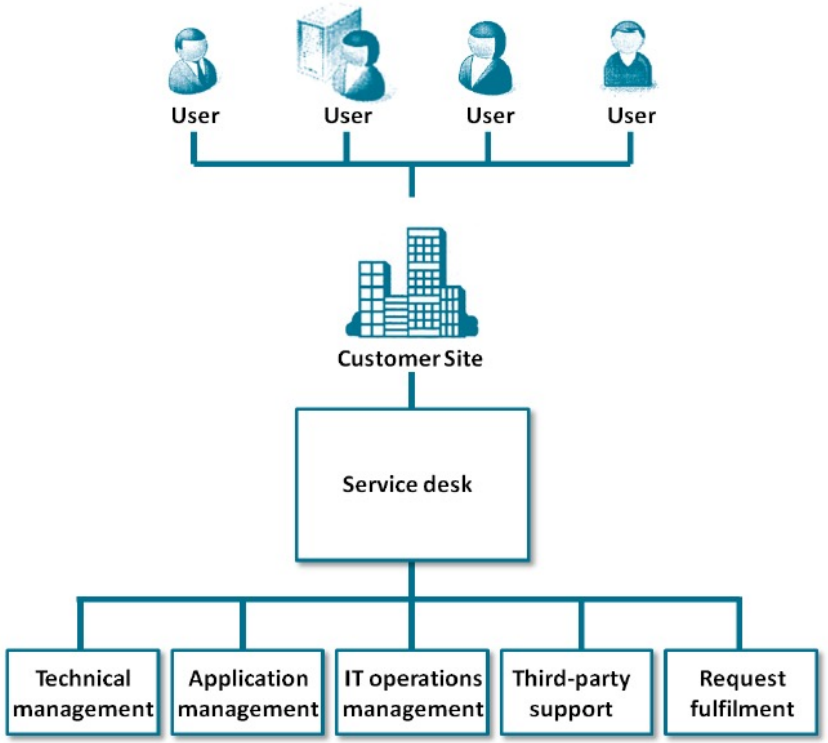
SUPPORTING TECHNOLOGIES

Structures of Service Desk

- Centralized
- Local
- Virtual
- Follow the Sun

SERVICE DESK STRUCTURE

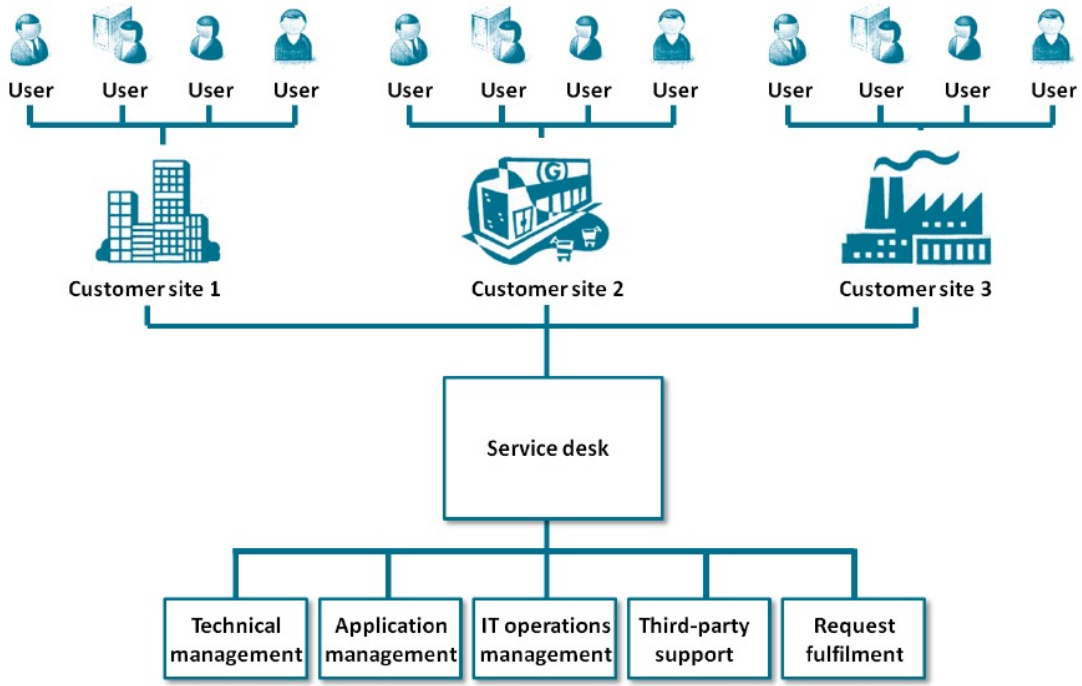
LOCAL



Users and support staff are located on the same premises or campus

SERVICE DESK STRUCTURE

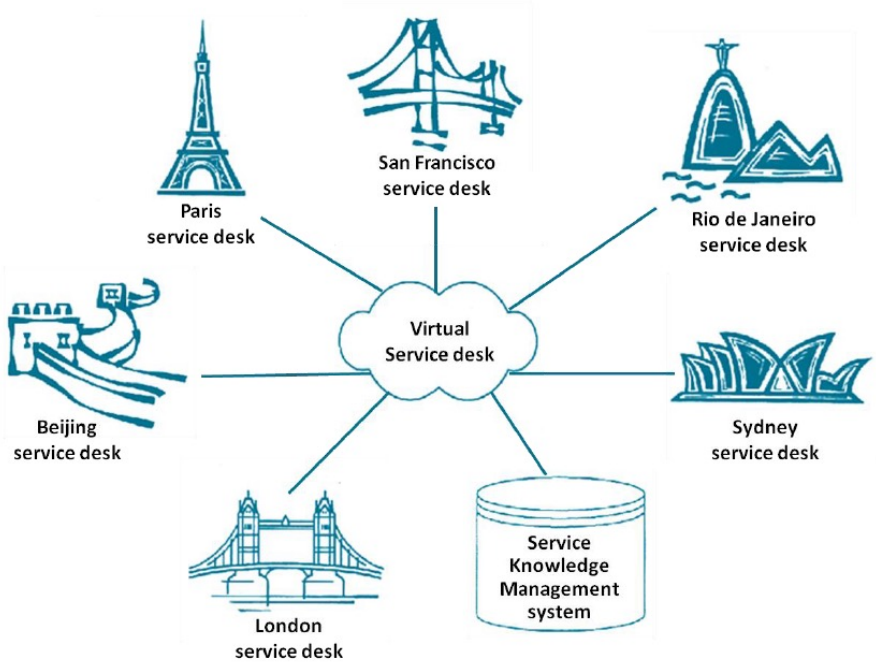
CENTRALIZED



Multiple user locations are serviced by a single support location

SERVICE DESK STRUCTURE

VIRTUAL



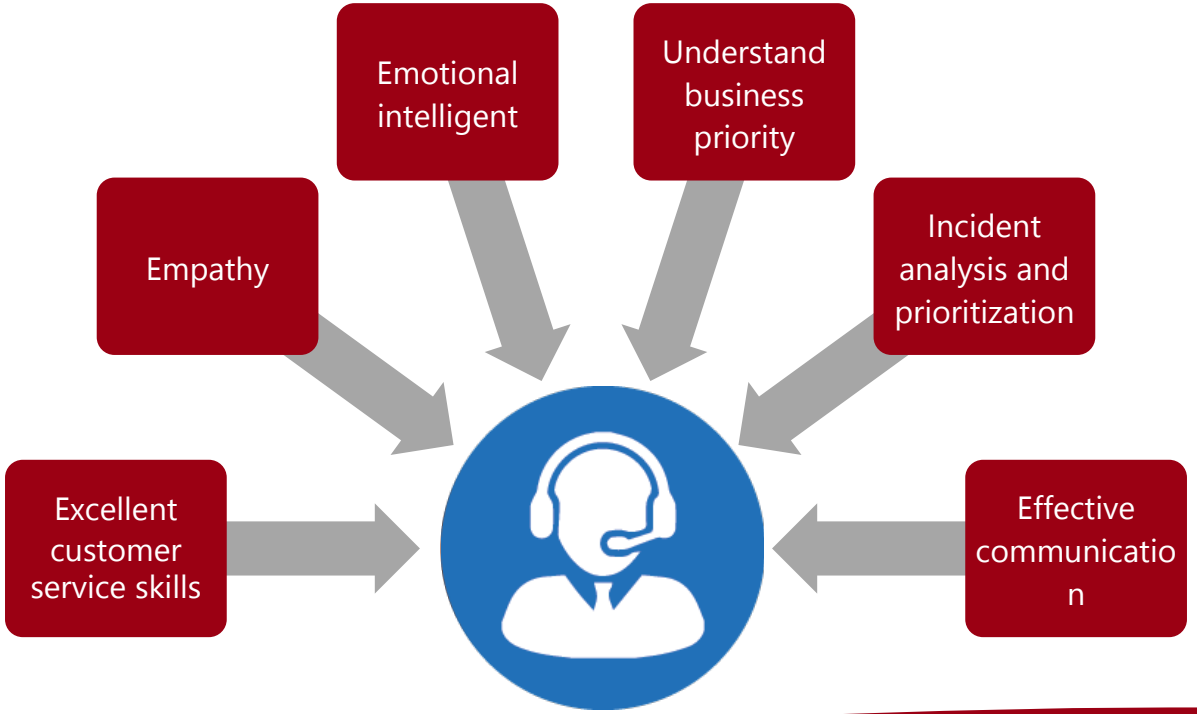
Virtual

Multiple user locations are serviced by multiple support locations which by virtue of call routing and other technology are able to appear and respond to user requests as a single entity

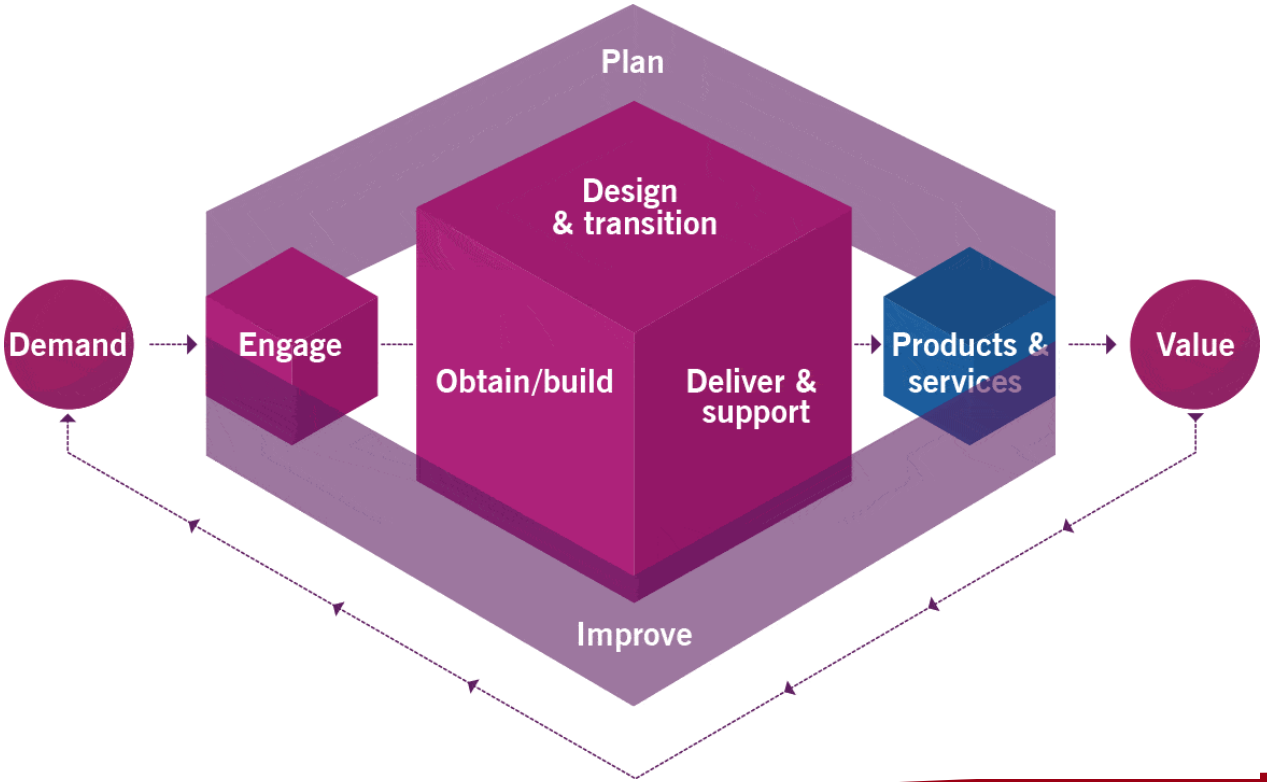
Follow the Sun

Identical to a virtual service desk, but organized in such a way as to utilize support staff shifts working during normal daylight hours for all user requests coming from any time zone

Service Desk Staff



SERVICE VALUE CHAIN



SERVICE DESK

Plan	Uninvolved
Improve	Monitoring and evaluating for continual improvement of service desk practice
Engage	Focuses on engaging with users and address their requests, queries and resolve incidents
Design & Transition	Involvement of the service desk to communicate the new or changed services to users
Obtain / Build	Acquiring the service components required for fulfilling service requests and resolving incidents
Deliver & Support	Coordinating for receiving, logging, resolving the incidents and queries of the users

IT Asset Management (ITAM)

to plan and manage the entire life-cycle of all the IT Assets, and ensuring:

- maximizing the value
- control costs
- manage risks
- enable decisions related to procurement
- utilization & retirement of assets
- meet contractual & regulatory requirements

IT Asset

any financially valuable component that can contribute to the delivery of an IT product or service

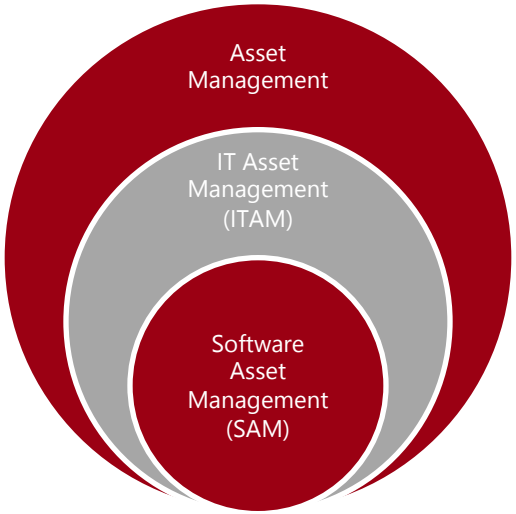
TYPES OF ASSET MANAGEMENT

IT Hardware Asset Management (IT HAM)

is a sub-practice of asset management that is specifically aimed at managing the lifecycles and total costs of IT equipment and infrastructure

Software Asset Management (SAM)

is an aspect of IT asset management specifically aimed at managing the acquisition, development, release, deployment, maintenance, and eventual retirement of software assets



- **SAM** procedures provide effective management, control, and protection of software assets

IT ASSET MANAGEMENT

- Understanding the **cost** and **value** of assets is essential
- **IT Asset Management** contributes to the visibility of assets and their value, which is a key element to successful service management
- **IT Asset Management** requires accurate inventory information, which it keeps in an **asset register**: it can be gathered in an audit, but it is much better to automate the collection of information
- The organization **needs to ensure** that the full lifecycle of each asset is managed, including **managing asset provisioning**; receiving, decommissioning, and return; hardware disposal; software re-use; leasing management; and potentially many other activities

IT ASSET MANAGEMENT

- **IT Asset Management** maintains the assets information, costs, and related contracts
- Therefore, the **IT asset register** is often combined (or federated) with the information stored in a configuration management system (CMS)
- In some organizations there is a centralized team responsible for **IT Asset Management**
- This **team** may also be responsible for configuration management
- Each organization must consider its own context and culture to choose the appropriate level of centralization

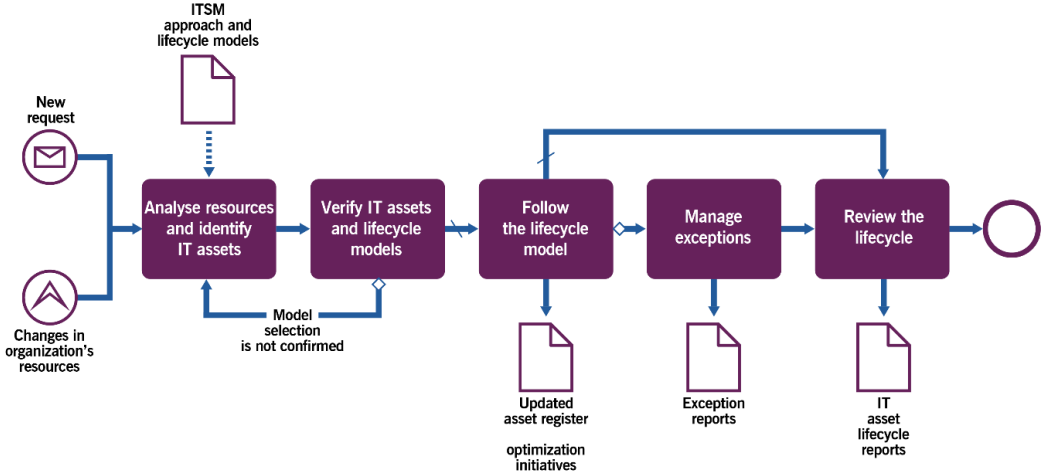
Activities

- **Hardware Assets** must be labelled for clear identification
- **Software Assets** must be protected from unlawful copying, which could result in unlicensed use
- **Cloud-based Assets** must be assigned to specific products or groups so that costs can be managed
- **Client Assets** must be assigned to individuals who take responsibility for their care

Activities

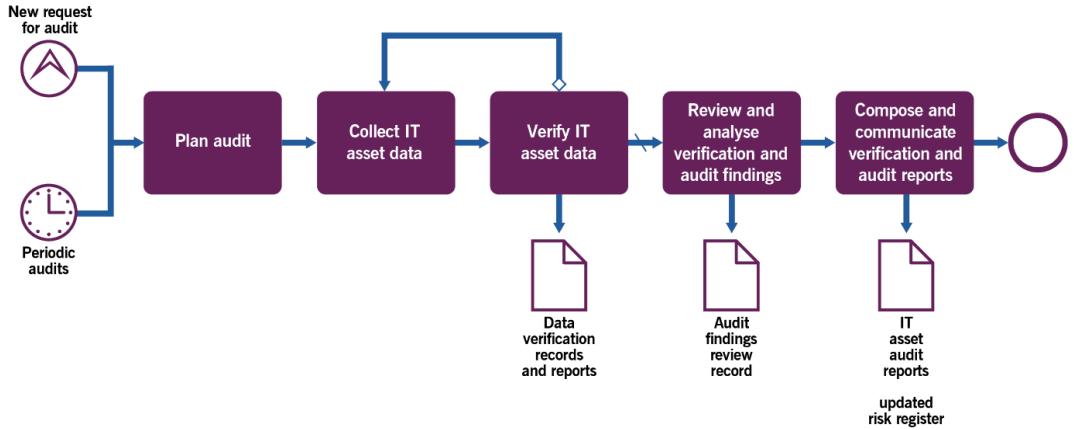
- **Define**, populate, and maintain the asset register in terms of structure and content, and the storage facilities for assets and related media
- **Control** the asset lifecycle in collaboration with other practices and record all changes to assets
- **Provide current** and historical data, reports, and support to other practices about IT assets
- **Audit assets**, related media, and conformity and drive corrective and preventive improvements to deal with detected issues

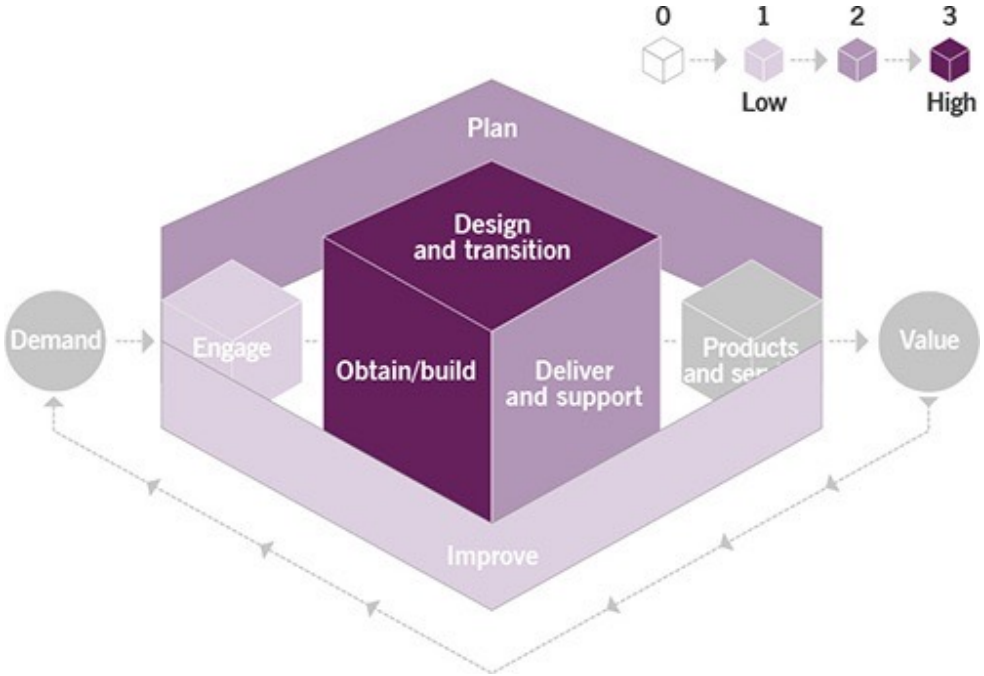
Workflow of the managing a common approach to ITAM process



Workflow of the managing the IT asset lifecycle and records process

Workflow for the verifying, auditing, and analysing IT assets process





Heat map of the contribution of IT asset management to value chain activities

IT ASSET MANAGEMENT

Plan	Most policies and guidance for IT asset management comes from the service financial management practice
Improve	Some improvements will directly involve IT asset management in helping to understand and manage costs
Engage	There may be some demand for IT asset management from stakeholders
Design & Transition	This value chain activity changes the status of IT assets
Obtain / Build	Ensure that assets are traceable from the beginning of their lifecycle
Deliver & Support	Locate IT assets, trace their movements, and control their status in the organization

Service Configuration Management

The purpose of the Service Configuration Management practice is to ensure that accurate and reliable information about the configuration of services, and the CIs that support them, is available when and where it is needed. This includes information on how CIs are configured and the relationships between them.

Configuration Item (CI)

any component that needs to be managed in order to deliver an IT service.

Service Asset

is any resources or capabilities that could contribute to the delivery of services

SERVICE CONFIGURATION MANAGEMENT

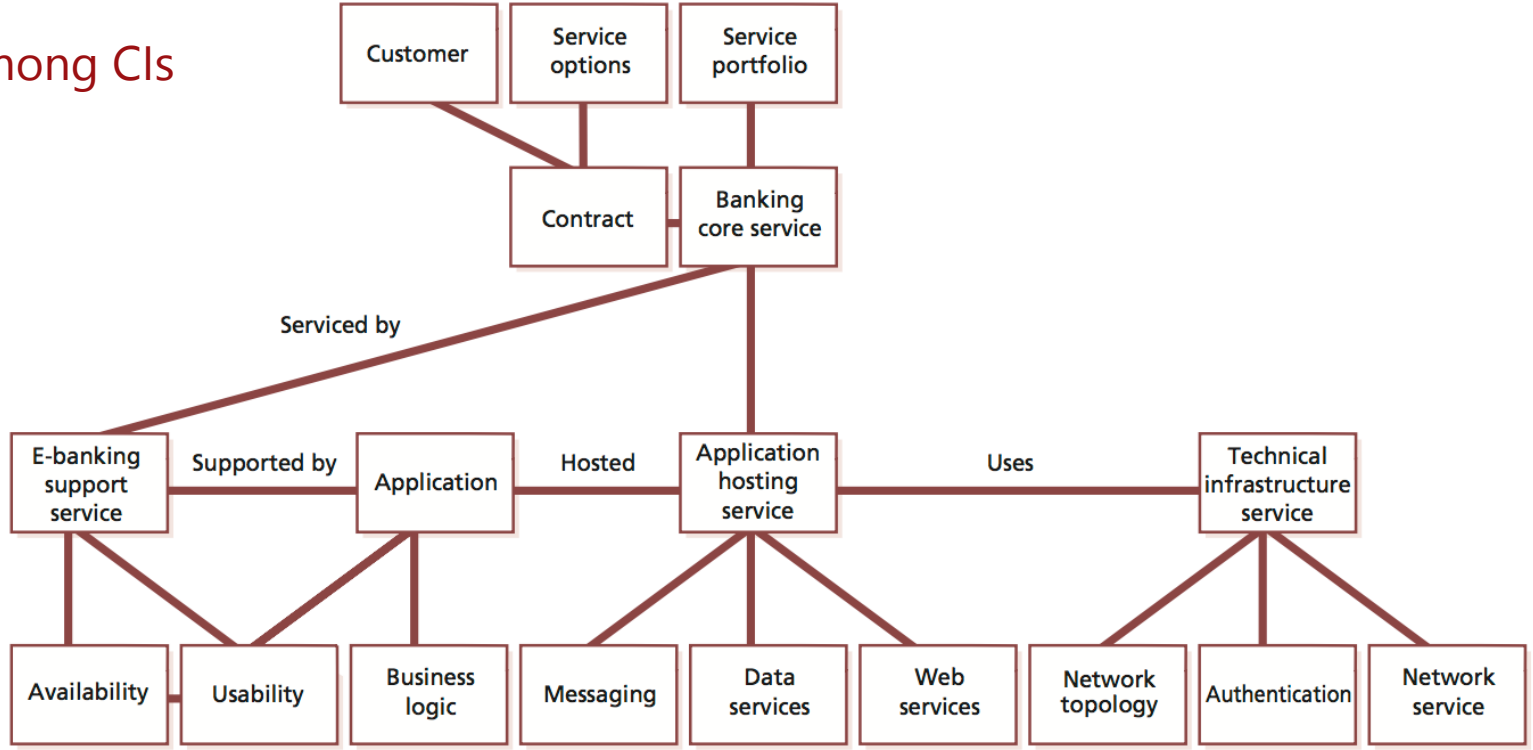
Each CI has:

- Category
- Attributes
- Relations
- Status

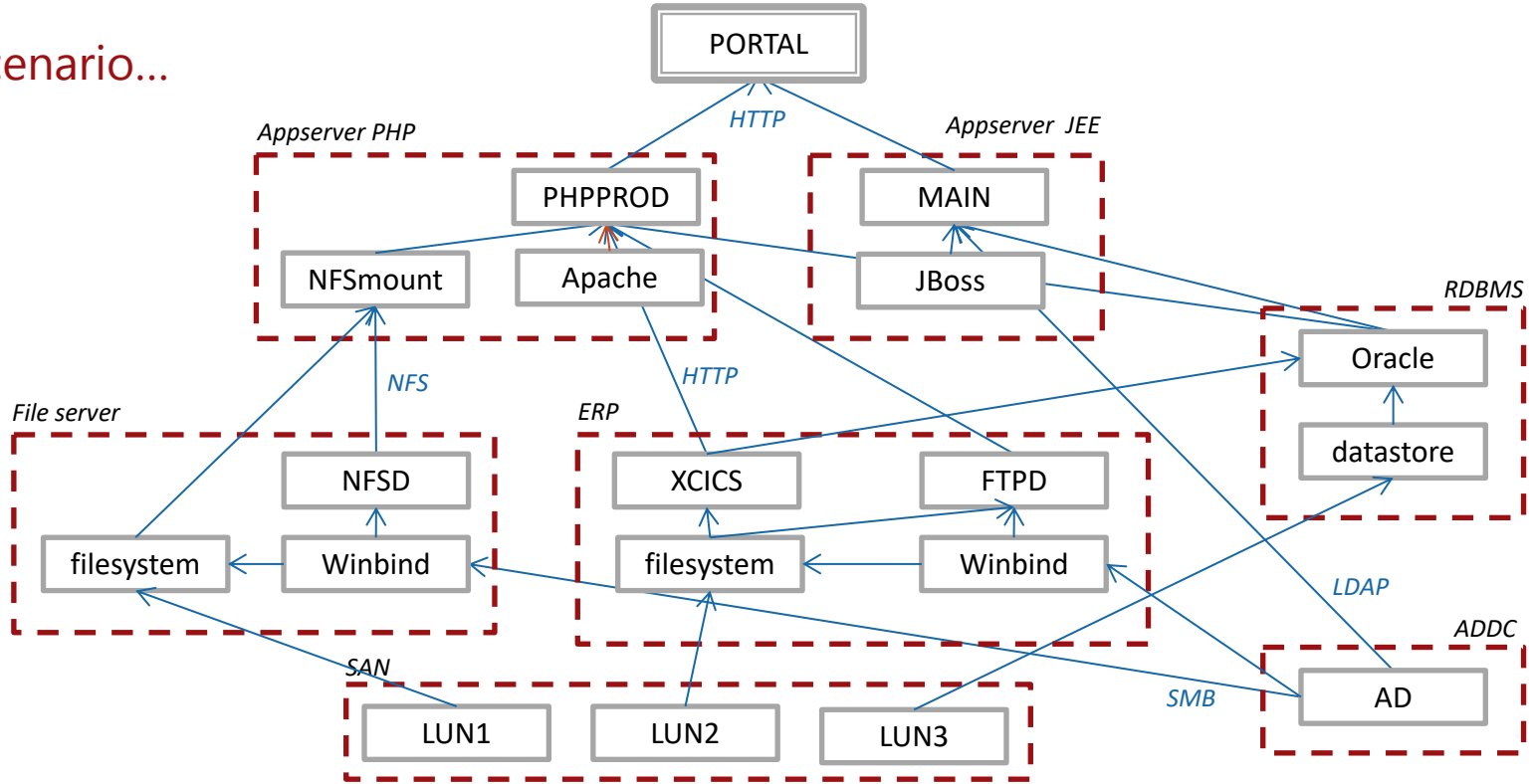
CI are always:

- Necessary to provide a Service
- Uniquely identifiable
- Subject to changes
- They can be managed

Relations among CIs

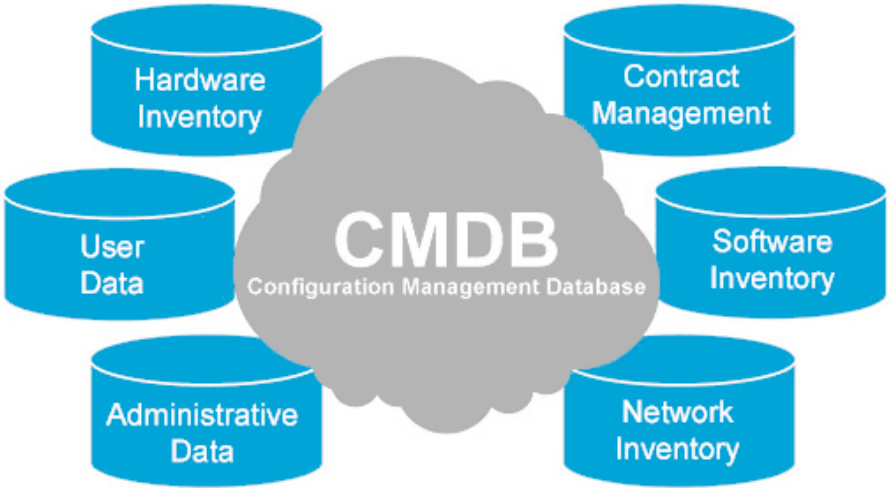


A real scenario…



Configuration Management DataBase (CMDB)

the minimum number of attributes and data that the CMDB should stores are as follows:

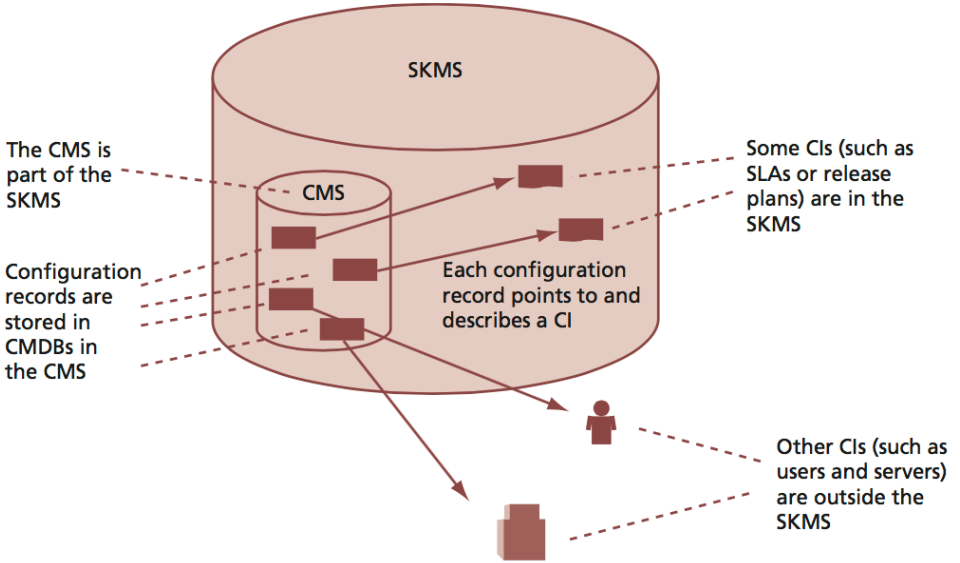


- CI Unique Identifier or Identification Code
- CI Name or Label (often, both, long names and short names)
- CI Abbreviations or Acronyms
- CI Description
- CI Ownership (organizations and people)
- CI Importance

Configuration Management System

a set of tools and database that are used to support service assets and manage IT Service Provider's Configuration data

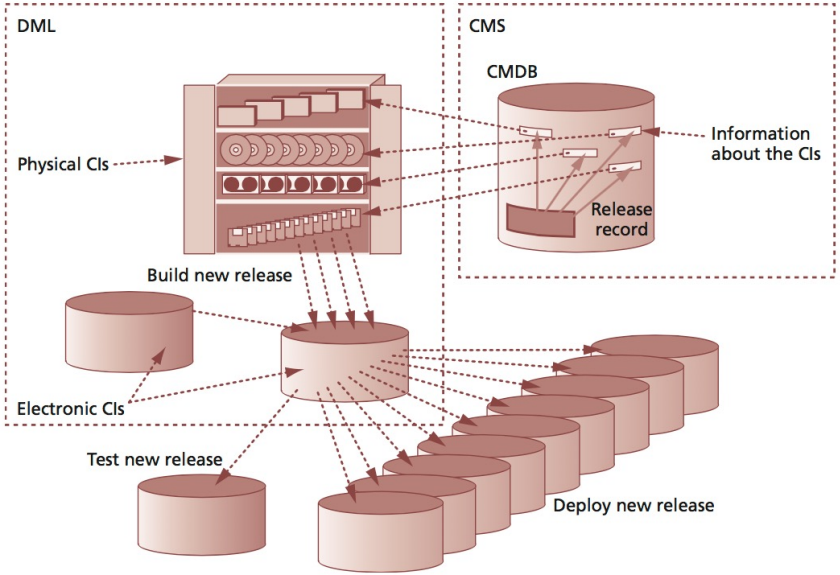
- In reality, you can see it as a set of different CMDBs
- The CMS includes information about Known Errors, Changes, and Releases and may contain data about employees, Suppliers, locations, Business Units, Customers, and Users
- CMS can also be integrated with other external databases of customers or suppliers for seamless information transfers



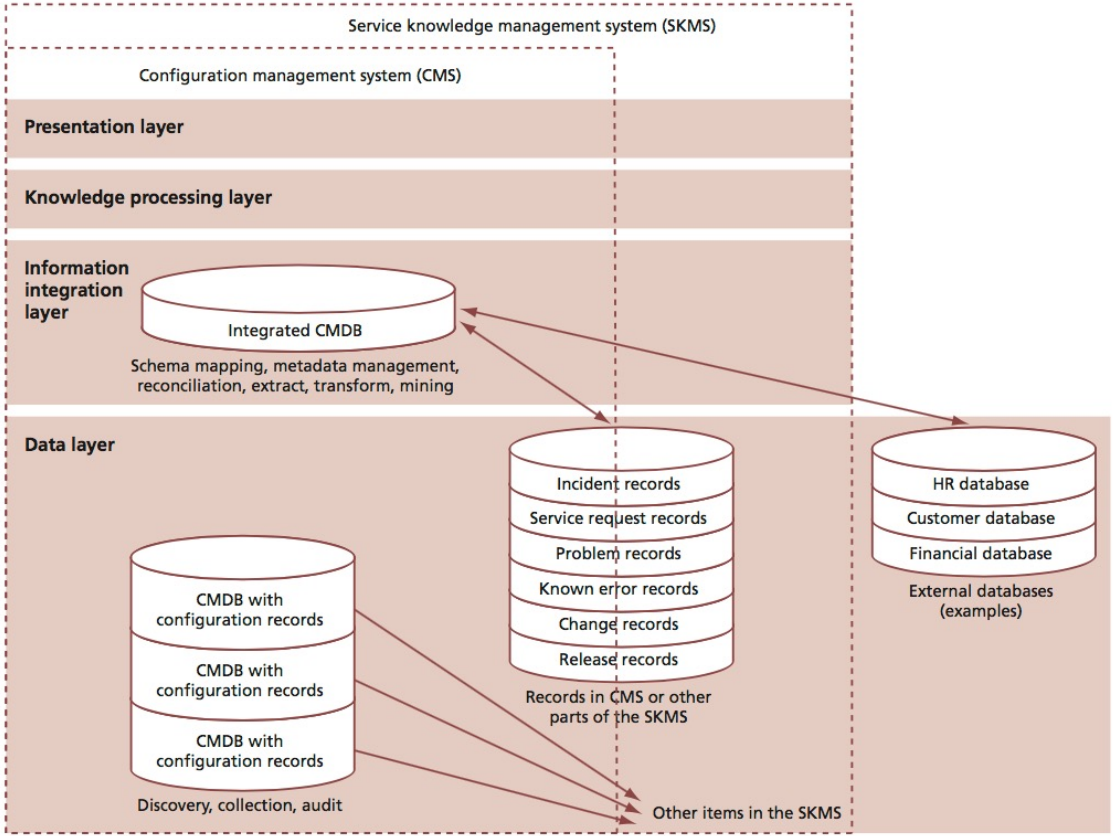
Definitive Media Library (DML)

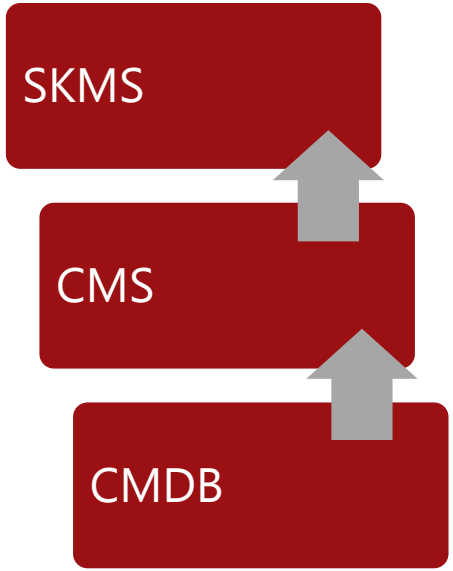
is the secure repository in which the definitive authorized versions of all media, software, license CIs are stored and protected

- It stores master copies of versions that have passed quality assurance checks and master copies of all controlled software in an organization
- DML is strictly controlled by SCM practice to ensure that only authorized media is stored
- DML may store data in the virtual storage or in physical storage (CD/DVD) or in both



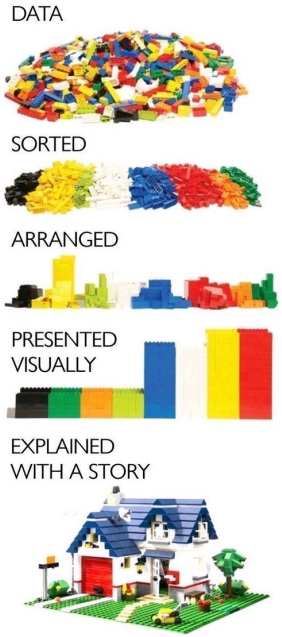
SERVICE CONFIGURATION MANAGEMENT

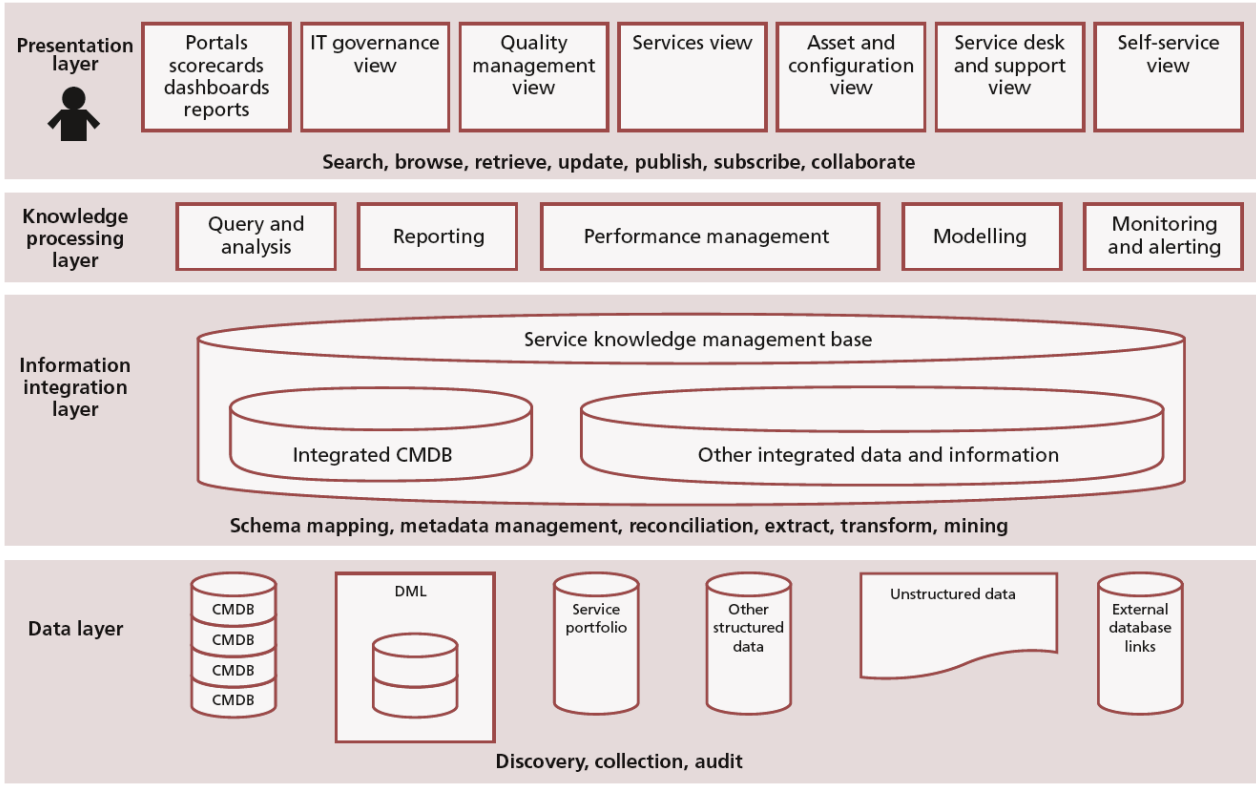




SERVICE CONFIGURATION MANAGEMENT

Service Knowledge Management System





Configuration Baseline

is the configuration of a service, product or infrastructure that has been formally reviewed and agreed, which thereafter serves as the basis for further activities and can be changed only through formal change procedures

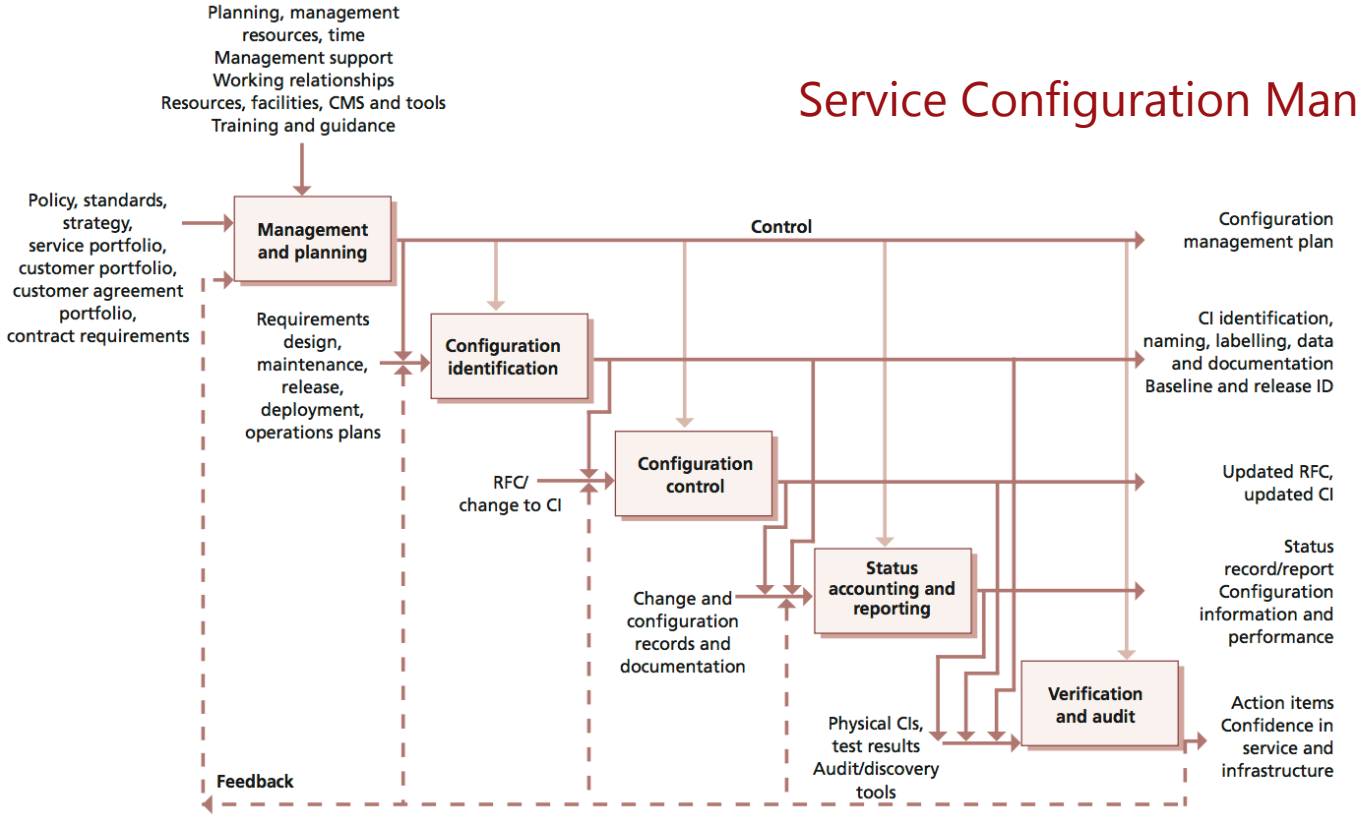
It captures the structure, contents and details of a configuration and represents a set of configuration items that are related to each other

Snapshot

is the current state of a configuration item or an environment, e.g. from a discovery tool

This snapshot is recorded in the CMS and remains as a fixed historical record

Service Configuration Management responsibility



SERVICE CONFIGURATION MANAGEMENT

Plan	Configuration management is used for planning new or changed services
Improve	Should be subject to measurement and continual improvement
Engage	There may be the require and use of configuration information from stakeholders
Design & Transition	Configuration management documents how assets work together to create a service
Obtain / Build	Configuration records may be created during this value chain activity, describing new or changed services and components
Deliver & Support	Information on CIs is essential to support service restoration

RELEASE MANAGEMENT

Purpose

to make new and changed services and features available for use

Release

a version of a service or other configuration item, or a collection of configuration items, that is made available for use

A **release** may comprise many different **infrastructure** and **application** components that work together to deliver new or changed functionality

It may also include **documentation**, **training**, **updated processes** or **tools**, and any other components that are required

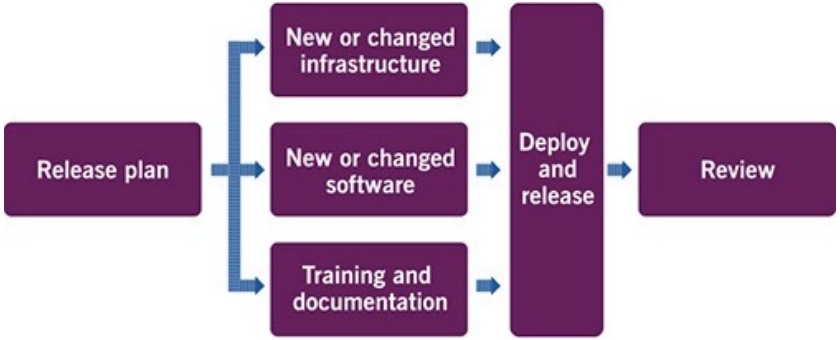
RELEASE MANAGEMENT

- **Releases** can range in size from the very small, to the very large
- In either case, a **Release Plan** will specify the exact combination of new and changed components to be made available, and the timing for their release
- A **Release Schedule** is used to document the timing for releases
- This **schedule** should be negotiated and agreed with customers and other stakeholders
- A **Release Post-Implementation Review** enables learning and improvement, and helps to ensure that customers are satisfied

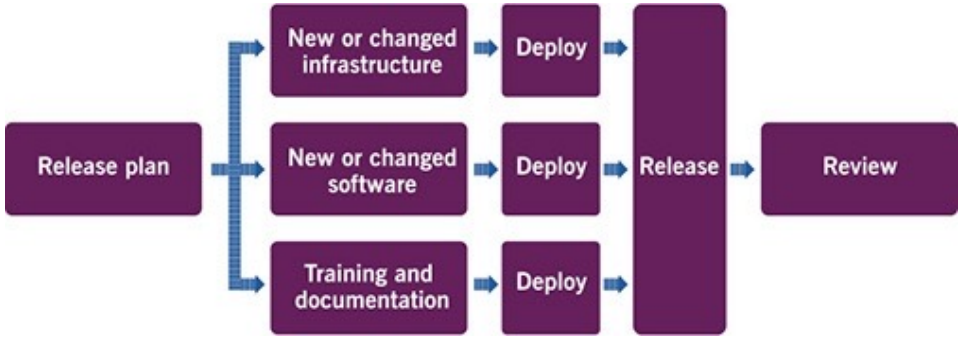
RELEASE MANAGEMENT

- In some **environments**, almost all release management work takes place before deployment, with plans in place as to exactly which components will be deployed in a particular release

- The **deployment** then makes the new functionality available



Release Management in a traditional/waterfall environment



Release Management in an Agile/DevOps environment

RELEASE MANAGEMENT

- **Release Management** is often staged, with pilot releases being made available to a small number of users to ensure that everything is working correctly before the release is given to additional groups

- Sometimes a **Release** must be made available to all users at the same time, as when a major restructuring of the underlying shared data is required

STAGING OF A RELEASE

Blue/green releases use two mirrored production environments

- Users can be switched to an environment that has been updated with the new functionality by using network tools that connect them to the correct environment

Feature flags enable specific features to be released to individual users or groups in a controlled way

- The new functionality is deployed to the production environment without being released

RELEASE MANAGEMENT

- In a **DevOps environment**, release management is often integrated with the continuous integration and continuous delivery toolchain
- The tools of **release management** may be the responsibility of a dedicated person, but decisions about the release can be made by the development team
- In a more **traditional environment**, releases are enabled by the deployment of the components
- Each release is described by a release record on an **ITSM tool**
- Release records are linked to **CIs** and **change records** to maintain information about the release

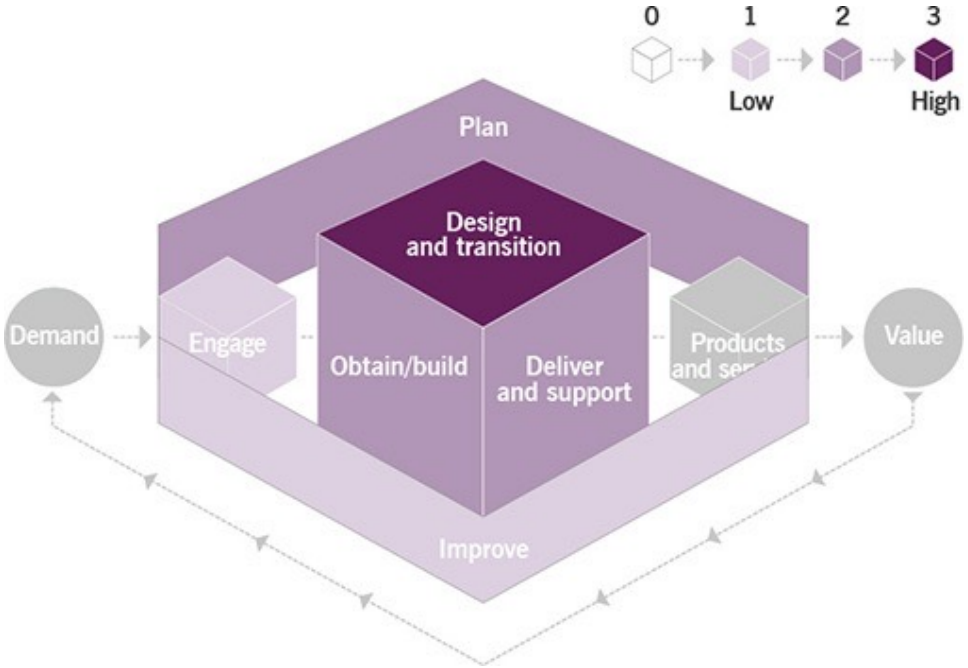
RELEASE MANAGEMENT

- **Third parties** often provide components of a **release**, like **cloud infrastructure**, **software as service** components, and **third-party support**
- It is also common to include **third-party software**, or **open-source software**, as part of application development
- **Release Management** needs to work across organizational boundaries to ensure that all components are compatible and to provide a seamless experience for users
- It also needs to consider the impact of changes to third-party components, and to plan for how these will be released

Activities include:

- Release policies and planning
- Release development and configuration design
- Acceptance of releases
- Rollout planning
- Extensive tests defined on the basis of acceptance criteria
- Communication, preparation and training
- Checking the HW and SW before and after the changes
- Installation of new HW or upgrade of the existing one
- Saving of the controlled SW both in centralized and distributed systems, distribution of the SW

RELEASE MANAGEMENT



Heat map of the contribution of IT release management to value chain activities

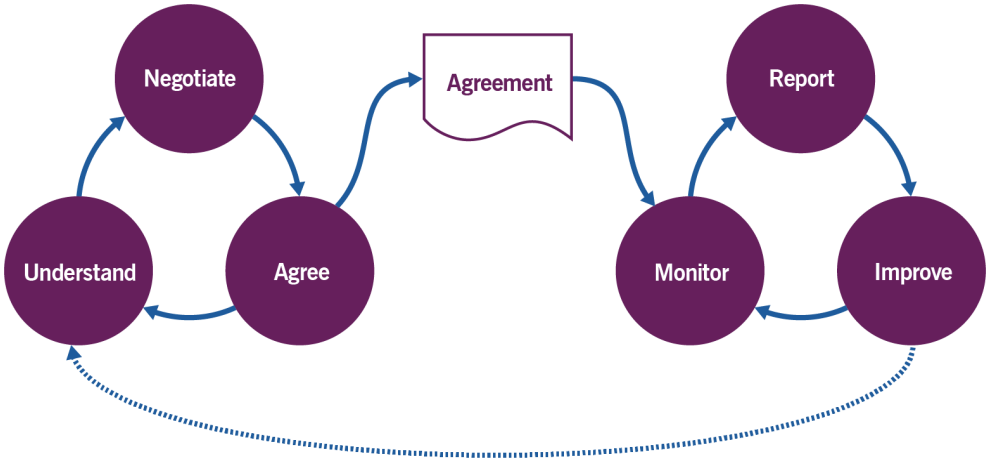
RELEASE MANAGEMENT

Plan	The organizational strategy and service portfolio drive policies, guidance, and timelines for releases / The size, scope, and content of each release should be planned and managed
Improve	New or changed releases may be required to deliver improvements, and these should be planned and managed in the same way as any other release
Engage	The content and cadence of releases must be designed to match the needs and expectations of customers and users
Design & Transition	Release management ensures that new or changed services are made available to customers in a controlled way
Obtain / Build	Changes to components are normally included in a release, delivered in a controlled way
Deliver & Support	Training, documentation, release notes, known errors, user guides, support scripts, etc. are provided by this practice to facilitate service restoration

Service Level Management

set clear business-based targets for services performance so that the delivery of a service can be properly assessed, monitored, and managed against these targets

Key activities of the Service Level Management practice (SLM)



Key activities of the Service Level Management practice (SLM)

- The service level management practice involves the definition, documentation, and active management of service levels

- It provides end to end visibility of the organization's services. For this, the service level management practice:
  - Establishes a shared view of the services and target service levels with customers
  - Ensures the organization meets the defined service levels
  - Performs service reviews
  - Captures and reports on service issues including performance against defined service levels

SERVICE LEVEL AGREEMENTS

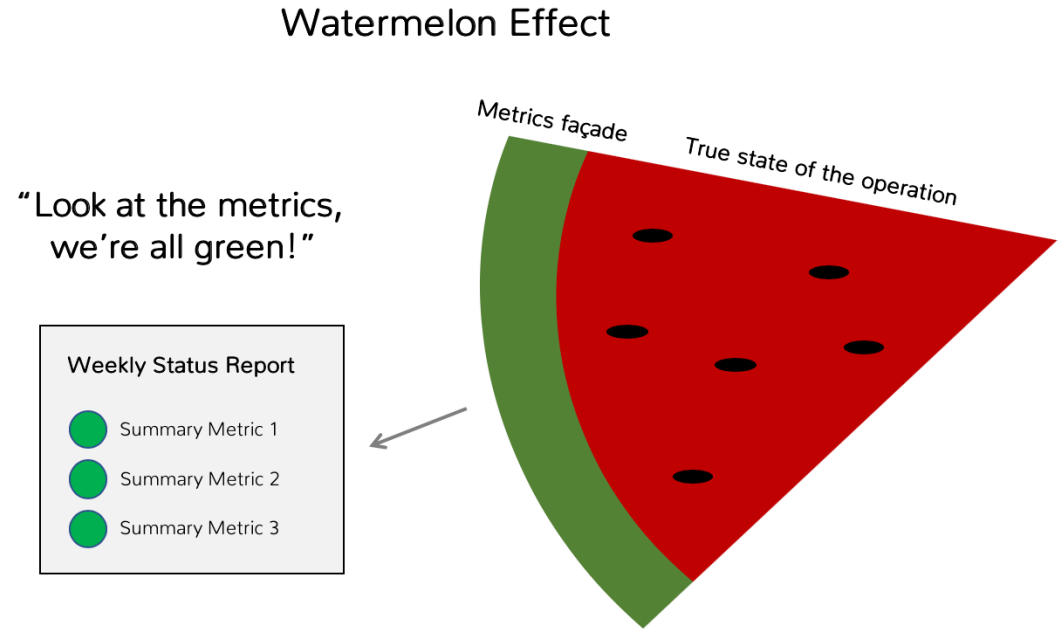
Service Level Agreement

a documented agreement between a service provider and a customer that identifies both services required and the expected level of service

- Service level agreements (SLAs) have long been used as a tool to measure the performance of services from the customer's point of view, and they must agree in the broader business context
- Using SLAs may present many challenges; often, they do not fully reflect the more comprehensive service performance and the user experience

The watermelon SLA Effect

In many cases, using single system-based metrics as targets can result in misalignment and a disconnect between service partners as to the success of the service delivery and the user experience



Requirements of Service Level management (SLM)

- Focus and effort to engage and listen to the requirements, issues, concerns, and daily needs of customers
- Engagement is needed to understand and confirm the actual ongoing needs and requirements of customers
- Listening is important as a relationship-building and trust-building activity, to show customers that they are valued and understood

Sources for Collating and analyzing Information

Customer engagement

involves initial listening, discovery, and information capture

Customer feedback

Surveys: from immediate feedback such as follow-up questions to incidents

Key business-related measures: measures agreed between the service provider and its customer, based on what the customer values as important

Operational metrics

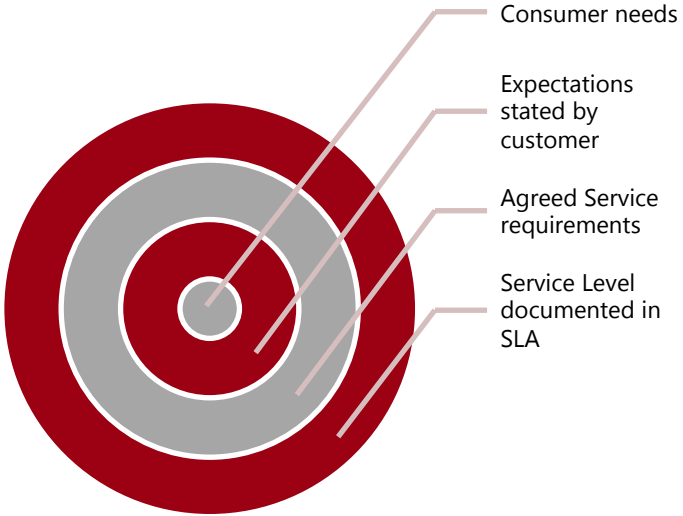
low-level indicators of various operational activities

Business metrics

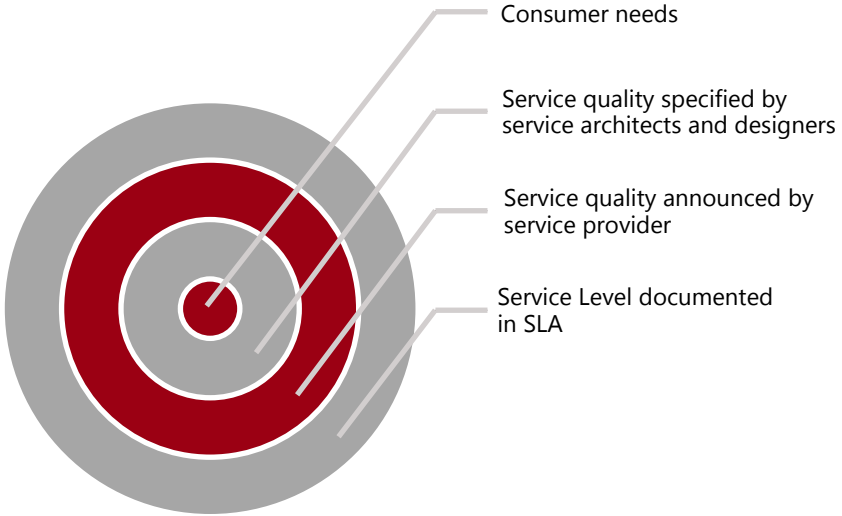
any business activity that is deemed useful or valuable by the customer

Practice success factors

Establishing a shared view of target service levels with customers

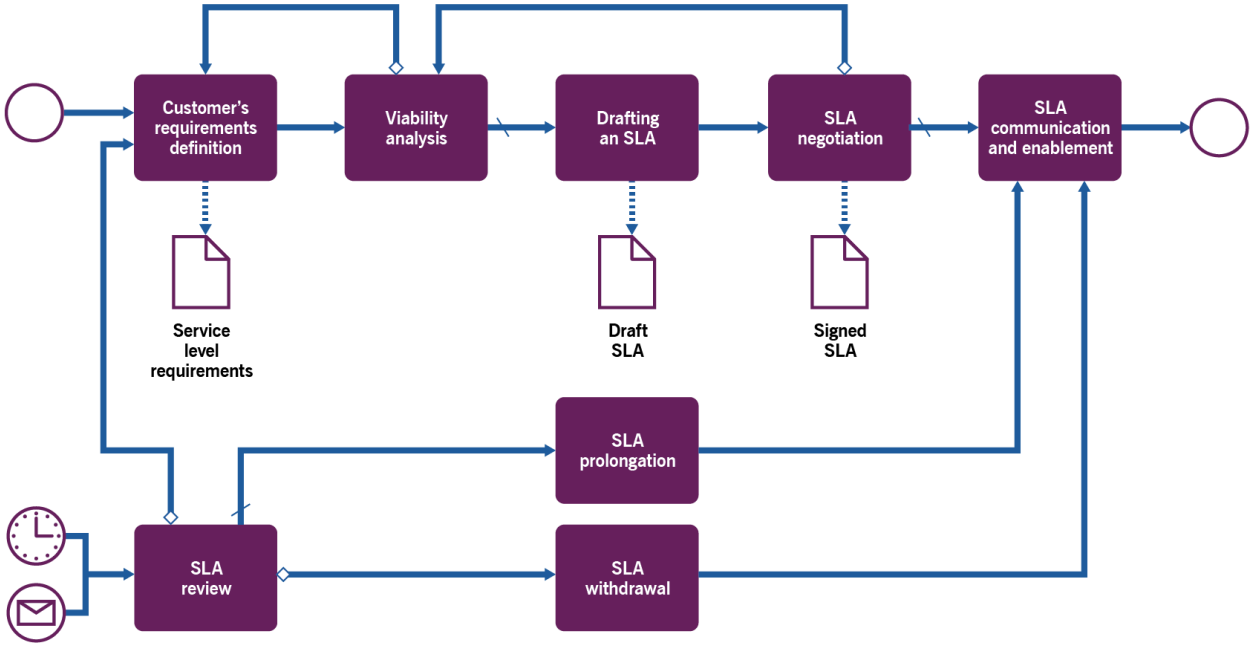


Tailored services: from customer needs to SLA

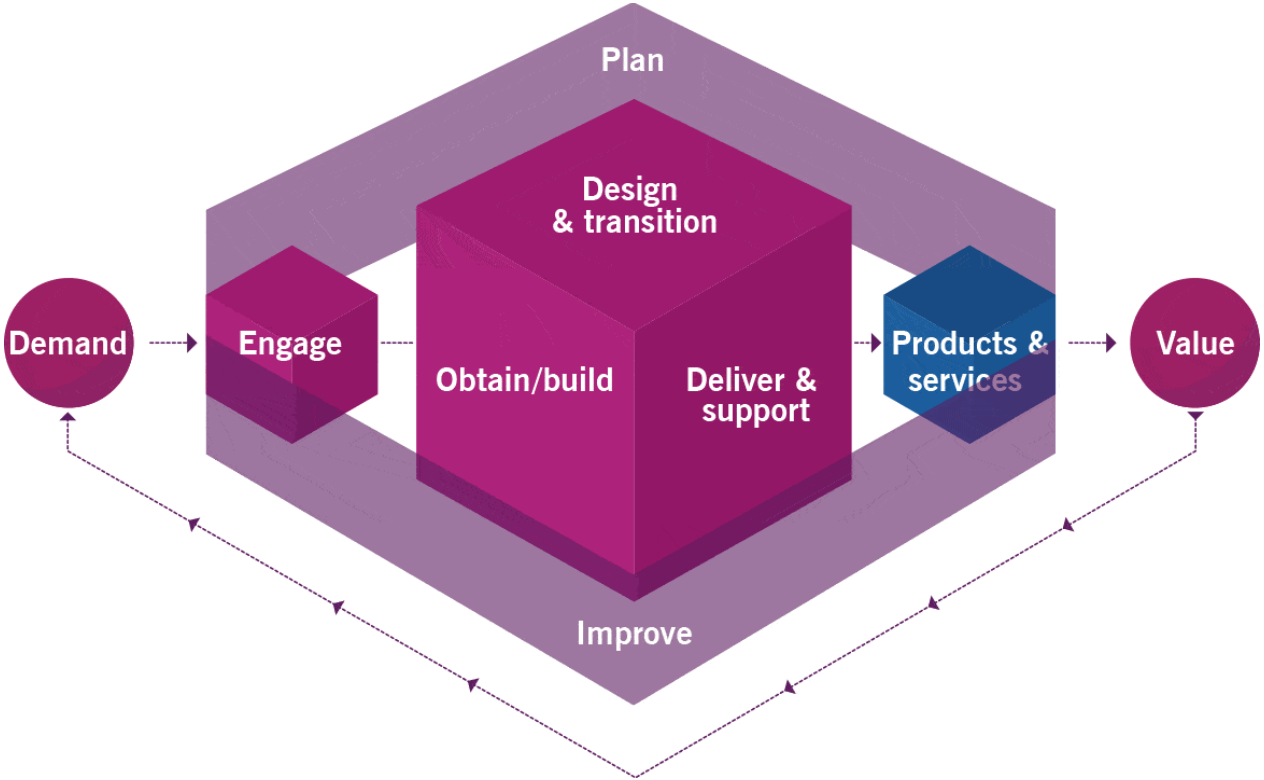


Out-of-the-box services: from consumer needs to SLA

Workflow for management of SLAs



SERVICE VALUE CHAIN



SERVICE LEVEL MANAGEMENT

Plan	Support planning of product and service portfolio and service offerings
Improve	SLM is a driving force for service improvement
Engage	Ensure ongoing engagement with customers and users through feedback
Design & Transition	Provide an input into the design of new and changed services
Obtain / Build	Receive objectives for components and service performance
Deliver & Support	Communicate service performance objectives to the operations and support teams

AVAILABILITY MANAGEMENT

Availability Management

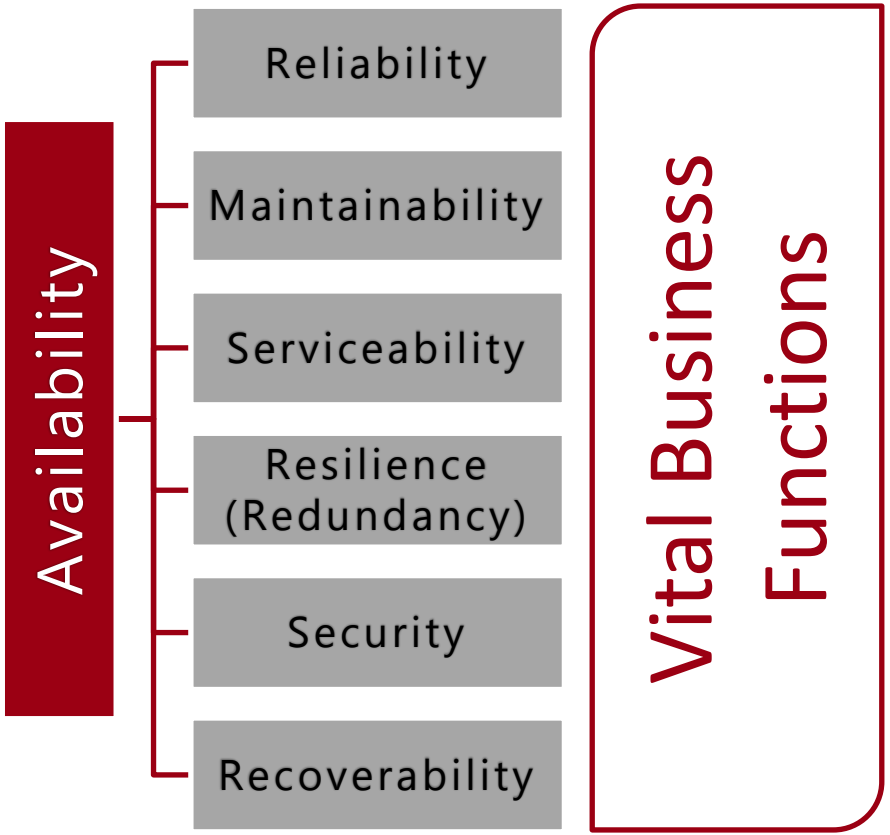
ensure that services deliver agreed levels of availability to meet the needs of customers and users

Availability

the ability of an IT service or other configuration item to perform its agreed function when required.

- negotiating achievable targets
- designing infrastructure and applications
- ensure the measure of availability
- monitoring, analysing and reporting availability
- planning improvement to availability

AVAILABILITY MANAGEMENT



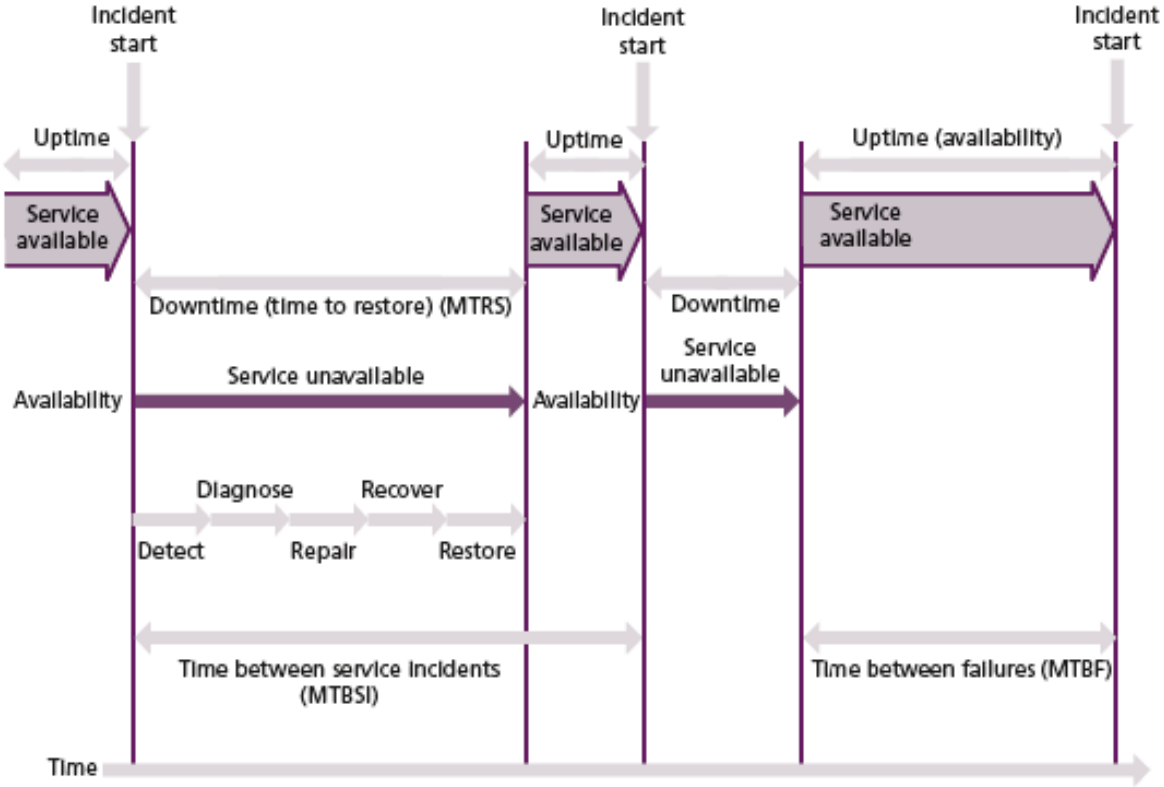
Availability is the ability of a service, component or CI to perform its agreed function when required

Note that down time should only be included in the following calculation when it occurs within the agreed service time (AST)

$$\text{Availability (\%)} = \frac{\text{Agreed service time (AST)} - \text{downtime}}{\text{AST}} \times 100$$

Incident LifeCycle

- Mean Time Between Failures
- Mean Time to Restore Service
- Mean Time Between Service Incidents
- Recovery Point Objective
- Recovery Time Objective



Availability Management rules

It is essential to establish the basic rules of Availability Management

- which vital business functions are affected by different application failures
- at what point is slow performance so bad that the service is effectively unusable
- when does the service need to be available, and when can the service provider carry out maintenance activities

IT and the Business must be sure they agree on the interpretation of the Availability metrics

Availability Management rules

The Customer's perception of downtime may differ from that of the IT department

- i.e., the "place of delivery" is their desk and not the IT department

When reporting availability data to the business, the language used by the business must be used

- For business, downtime means: unusable workforce, lost earnings, dissatisfied end customers, threats of legal action and the inability to comply with legislation

Both the total duration of the downtime and its frequency affect the quality of the service

Availability Management example 1

SLA: service running 5 days x 8 hours / week

The service was down for 4 hours during week 43, so availability was

(40-4) / 40x100 = 90%

It's not so simple: it depends on what has been agreed, how and what is measured, how many etc.

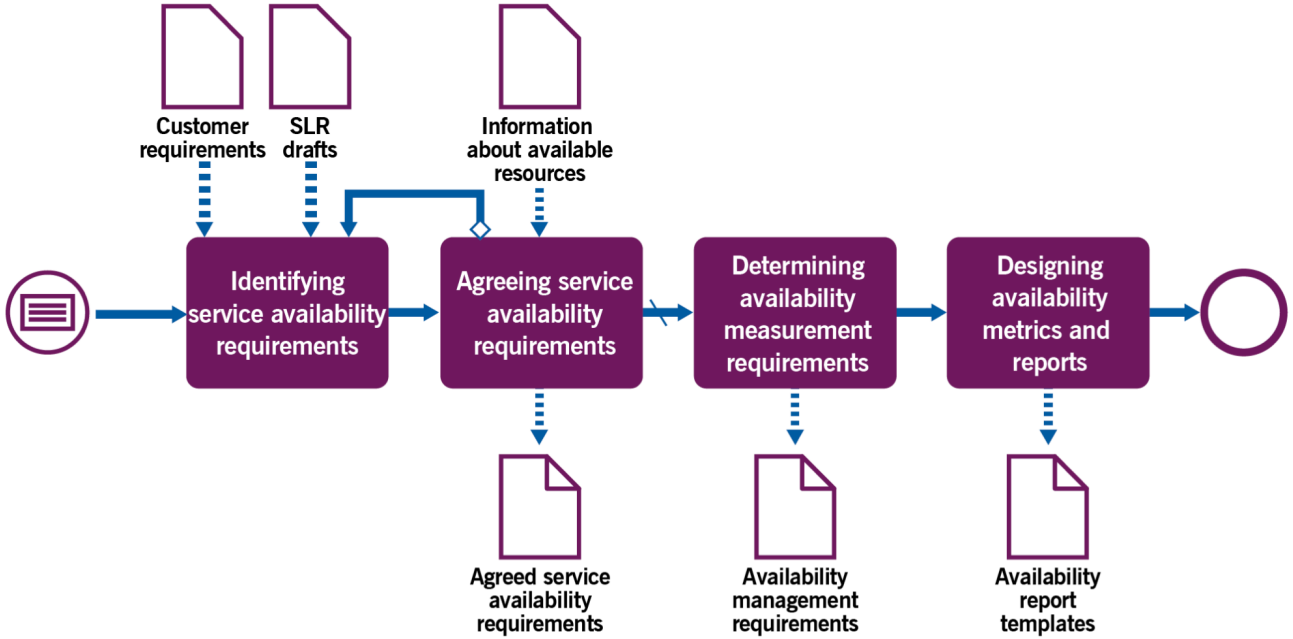
If only one of the 1000 users has a downtime of 4 hours, can we really talk about 10% downtime or should it be considered 10/1000 = 0.01%?
For that user it is 10% but for the whole company it is much less

Availability Management example 2

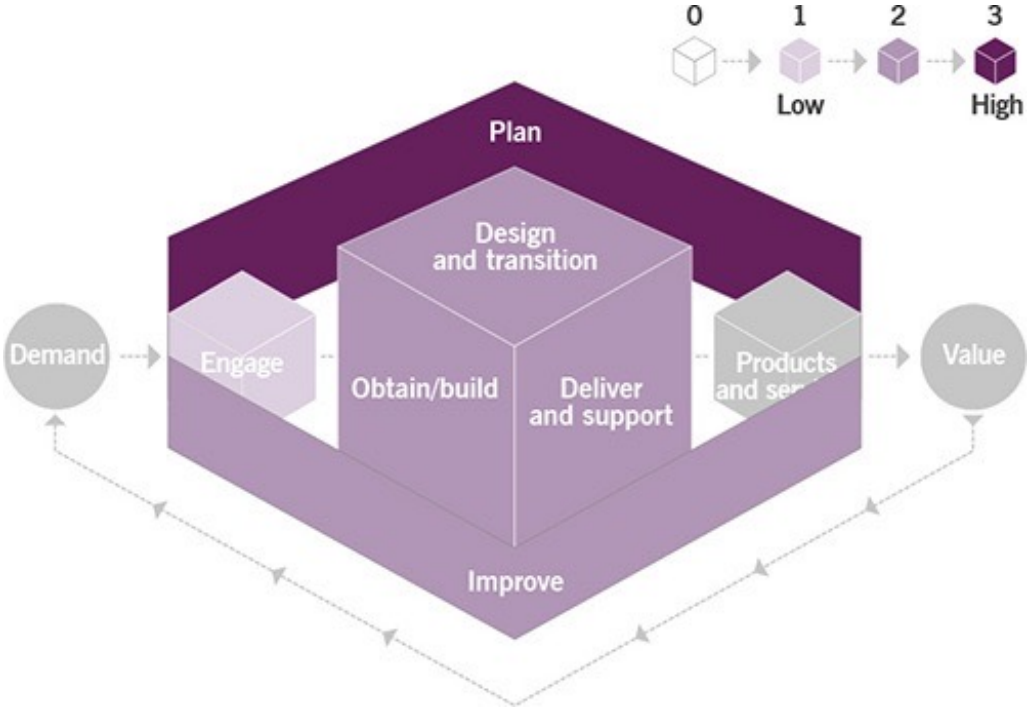
Even when the SLA is met, the service can be perceived as unavailable

i.e. an Invoicing Application is used by the Finance division from Monday to Friday from 9:00 to 17:00. Every day, from Monday to Friday, between 20:00 and 22:00, the backup is made (which makes it unavailable).
The backup schedule has been agreed with the customer and it was written in the SLA.
A Finance user works overtime: at 20:00 he loses his access to the application due to the backup in progress. For the user, the service is not available, while the SLA has not been broken.

Workflow for the establishing Service Availability Control Process



AVAILABILITY MANAGEMENT

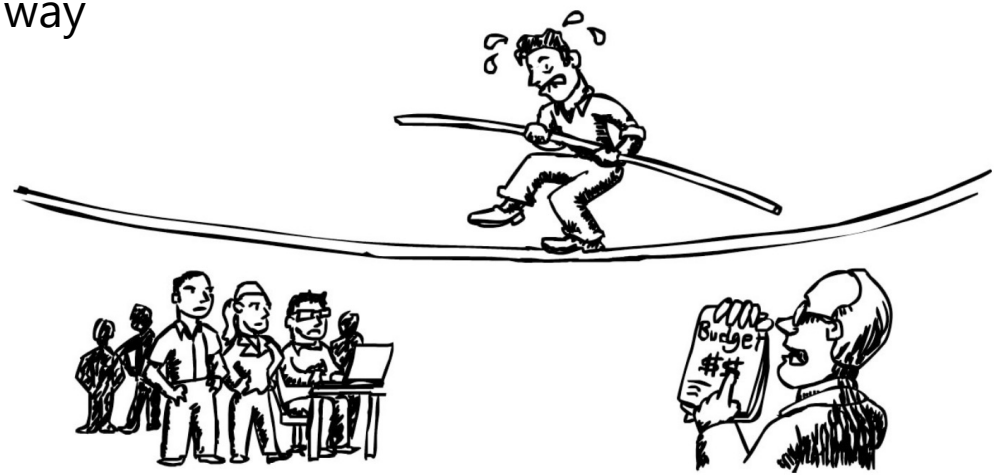


Heat map of the contribution of availability management to value chain activities

Capacity and Performance Management

ensure that services achieve agreed and expected performance, satisfying current and future demand in a cost-effective way

The purpose of this discipline is to ensure that there is always a reserve of IT capacity, the costs of which are justifiable and that meet the needs of the business.



Performance

a measure of what is achieved or delivered by a system, person, team, practice, or service

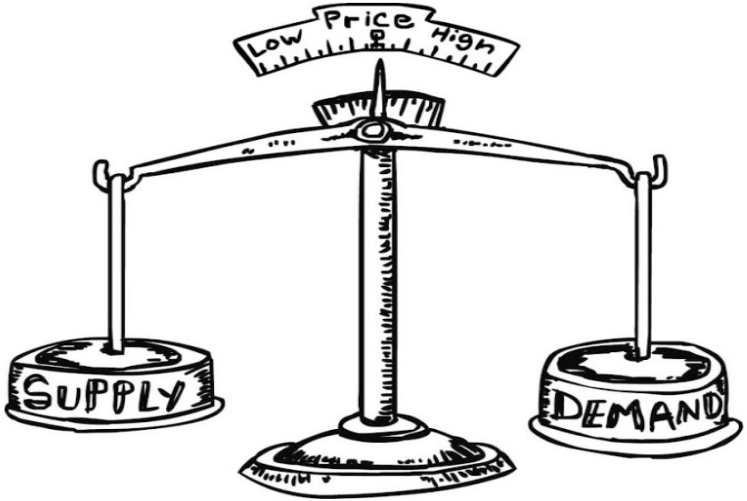
It determines business demand (in terms of IT resources), forecast workloads and schedule IT resources. One of the most important contributions of the process is to provide a well documented Capacity Plan.

Are you buying the right amount of infrastructure at the right time?

It includes the following activities:

- service performance and capacity analysis
  - research and monitoring of the current service performance
  - capacity and performance modelling
- service performance and capacity planning
  - capacity requirements analysis
  - demand forecasting and resource planning
  - performance improvement planning

Avoid overprovision



It is essentially a balancing act

CAPACITY AND PERFORMANCE MANAGEMENT

BUSINESS CAPACITY MANAGEMENT

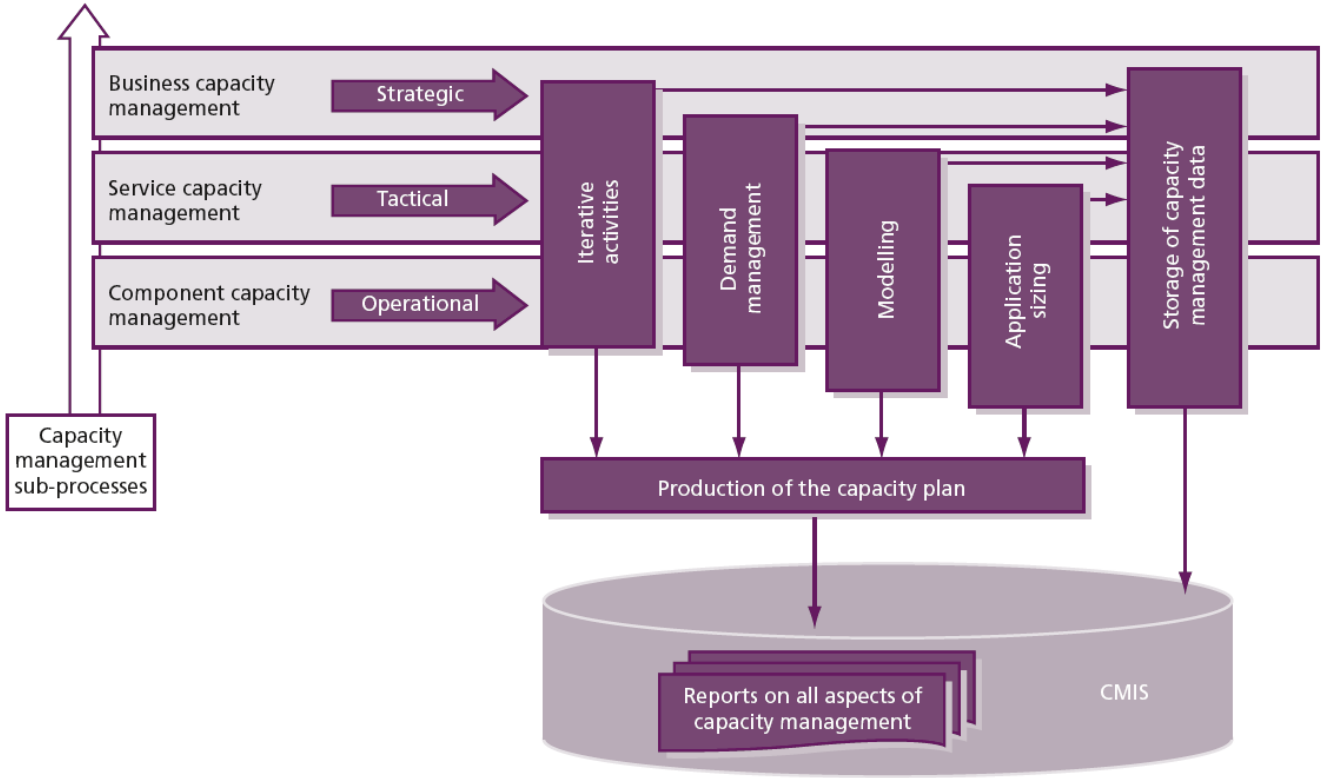
is focused on current and future business requirements

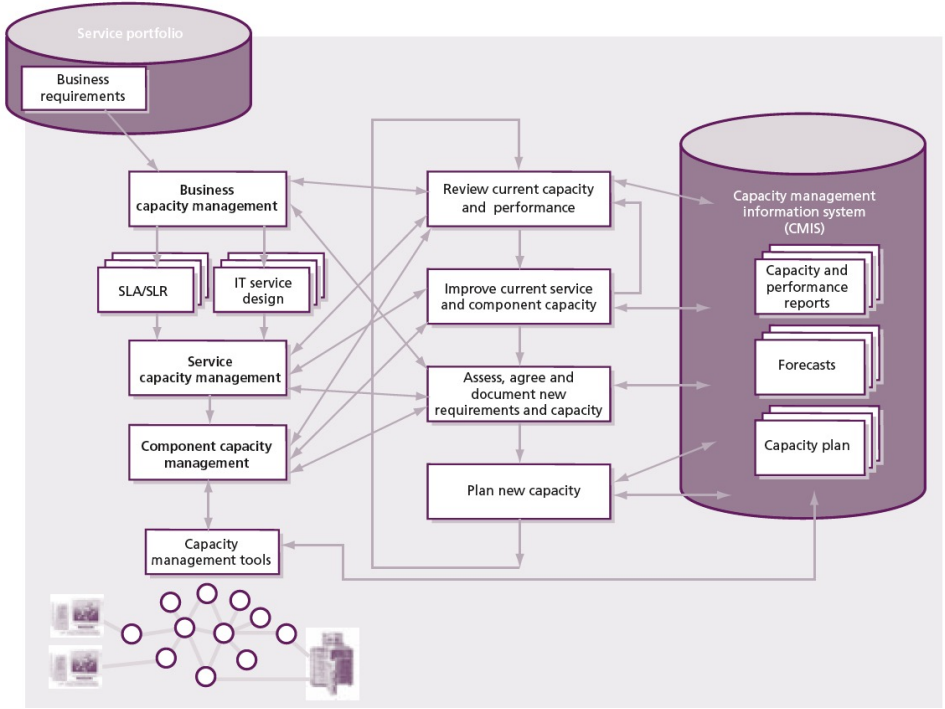
SERVICE CAPACITY MANAGEMENT

is focused on the provision of existing services that support the business

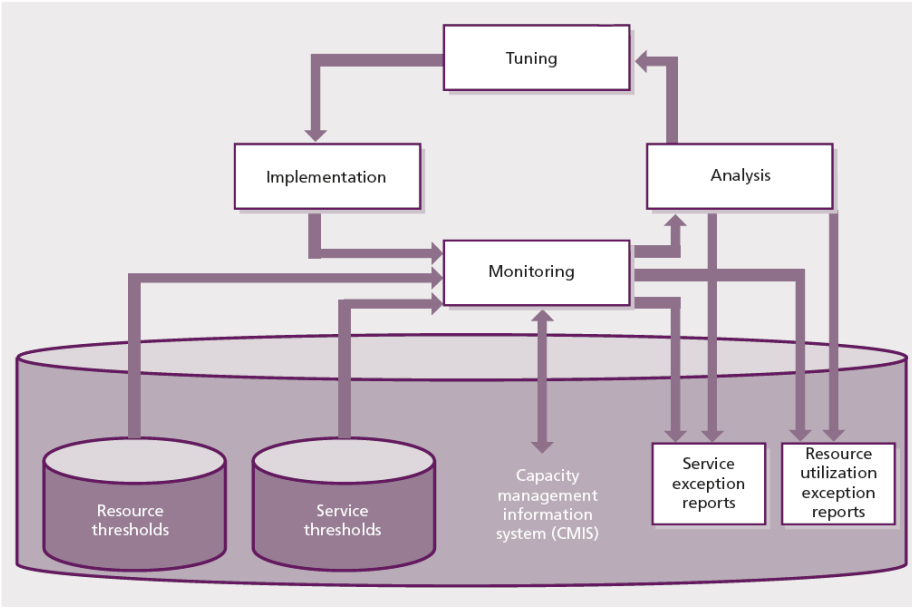
COMPONENT CAPACITY MANAGEMENT

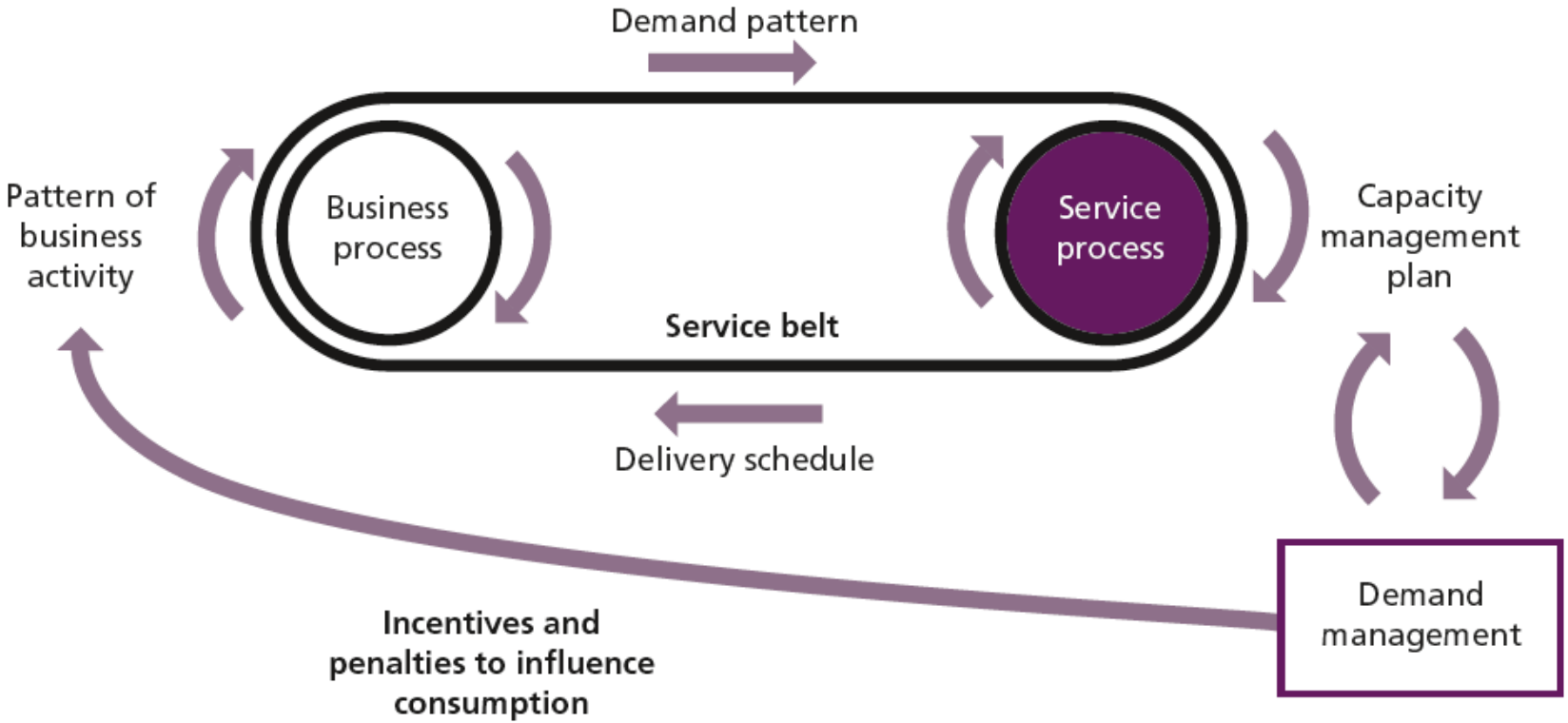
is focused on the technology underlying the provision of all services

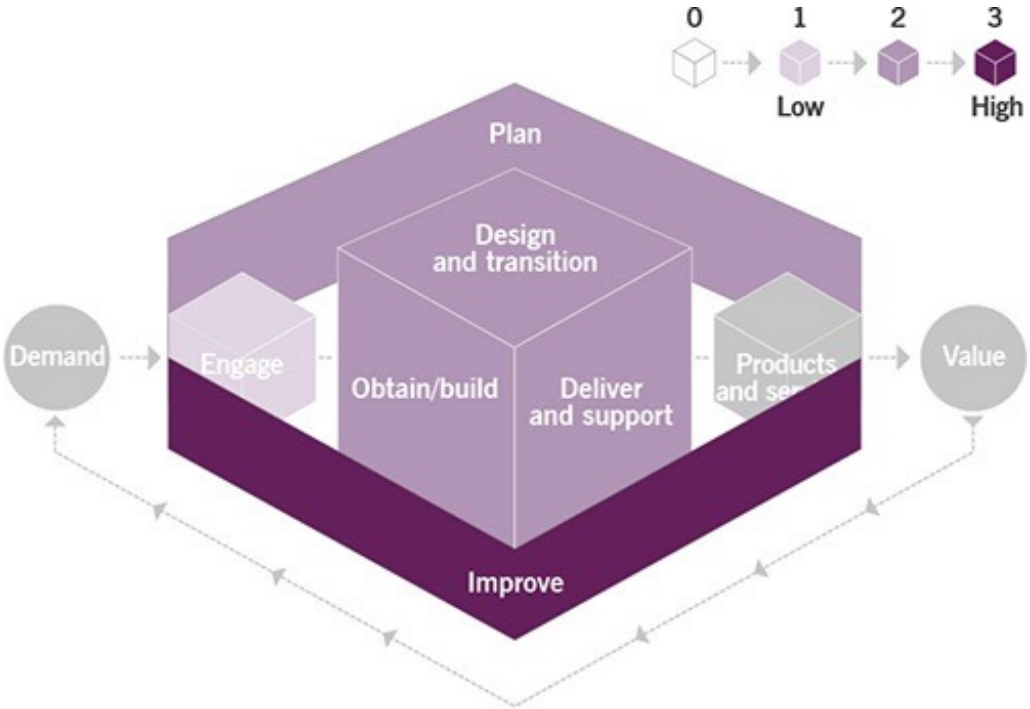

Business capacity management
Strategic
Service capacity management
Tactical
Component capacity management
Operational
Iterative activities
Demand management
Modelling
Application sizing
Storage of capacity management data
Capacity management sub-processes
Production of the capacity plan
Reports on all aspects of capacity management
CMIS



The ongoing iterative activities of capacity management




Demand pattern
Pattern of business activity
Business process
Service process
Capacity management plan
Service belt
Delivery schedule
Demand management
Incentives and penalties to influence consumption



Heat map of the contribution of capacity and performance management to value chain activities

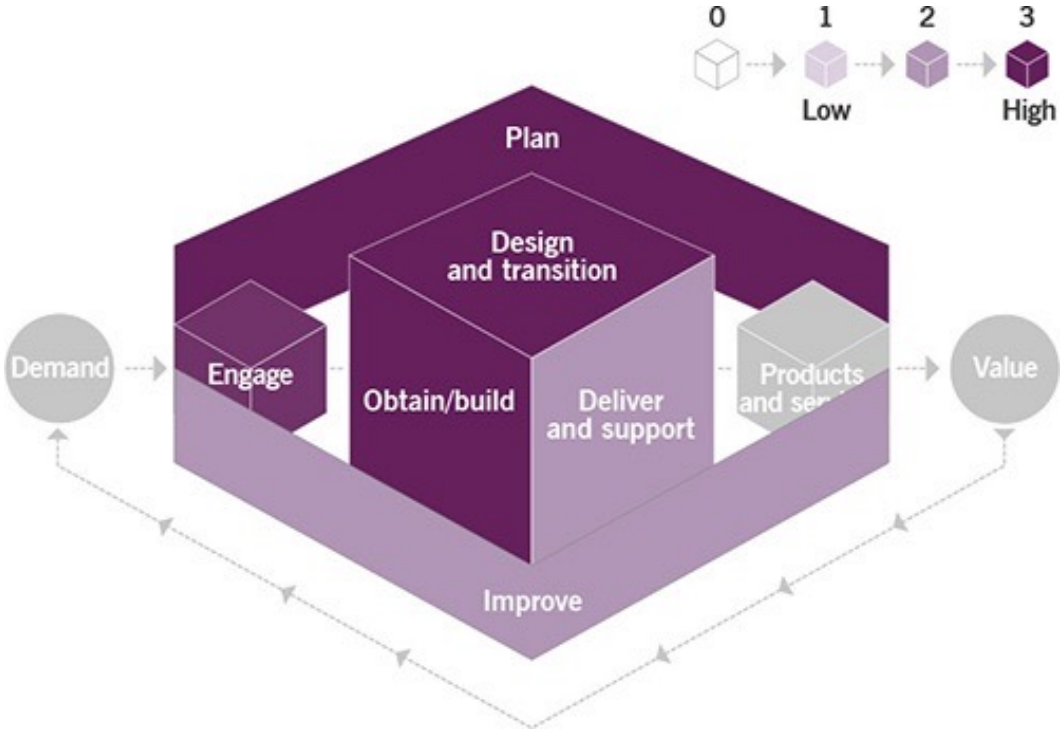
Business Analysis

analyse a business or some element of it, define its associated needs, and recommend solutions to address these needs and/or solve a business problem, which must facilitate value creation for stakeholders

Business analysis enables an organization to communicate its needs in a meaningful way, express the rationale for change, and design and describe solutions that enable value creation in alignment with the organization's objectives

The key activities associated with business analysis are:

- analysing business systems, business processes, services, or architectures in the changing internal and external context
- identifying and prioritizing parts of the SVS, and products and services that require improvement, as well as opportunities for innovation
- evaluating and proposing actions that can be taken to create the desired improvement
- documenting the business requirements for the supporting services to enable the desired improvements
- recommending solutions following analysis of the gathered requirements and validating these with stakeholders



Heat map of the contribution of business analysis to value chain activities

Service Continuity Management

ensure that the availability and performance of a service are maintained at sufficient levels in case of a disaster.

The practice provides a framework for building organizational resilience with the capability of producing an effective response that safeguards the interest of key stakeholders and the organization's reputation, brand and value-creating activities

Disaster

a sudden unplanned event that causes great damage or serious loss to an organization.

To be classified as a disaster, the event must match certain business-impact criteria that are predefined by the organization.

SERVICE CONTINUITY MANAGEMENT

A list of disasters generally includes:

- cyber attacks
- electricity outages
- failures of strategic partners
- fires
- floods
- key personnel unavailability
- large-scale IT infrastructure failures (such as data-centre failures)
- natural disasters

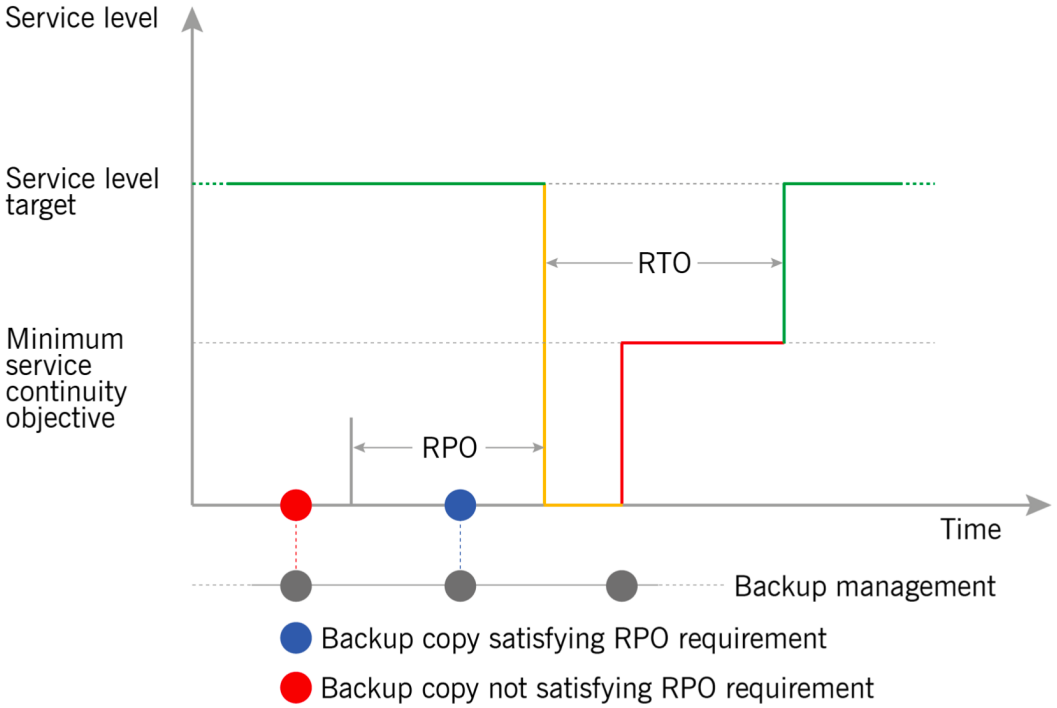
Defining those events which are not disasters is equally important.

The service continuity management practice includes the following areas:

- performing BIA to quantify the impact of service unavailability to the service provider and service consumers
- developing service continuity strategies (and integrating them into the business continuity management strategy, if relevant)
- developing and managing service continuity plans (and providing a clear interface to business continuity plans, if relevant)
- performing exercises and testing the service continuity plans invocation in case of disaster

* Business Impact Analysis (BIA) is a process of analysing activities and the effect that a disruption might have on them

SEVICE CONTINUITY MANAGEMENT

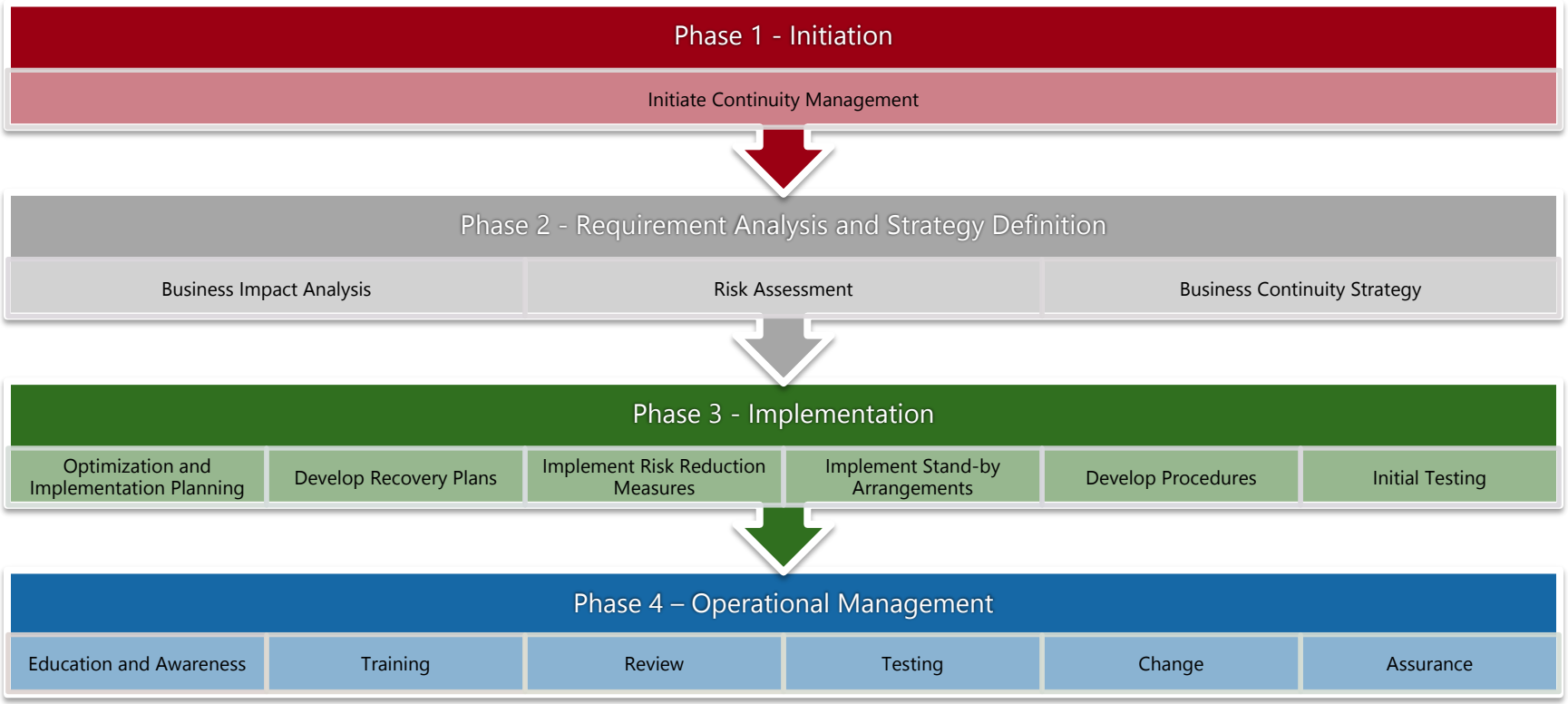


Recovery Time Objective (RTO)
is the targeted duration of time and a service level within which a business process must be restored after a disaster

Recovery Point Objective (RPO)
is the maximum targeted period during which transactional data is lost from an IT service due to a major incident.

Minimum Target Service Level
Is the level of service which is acceptable to the service provider to achieve its objectives during a disruption.

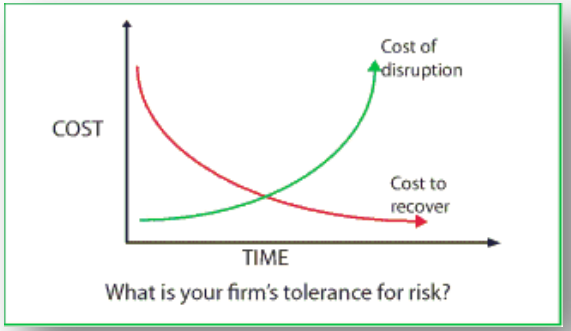
SERVICE CONTINUITY MANAGEMENT



The options

The choice of options usually depends a lot on the finances available or how much the business wants to invest.

Contingency Plan



Evaluate Your Firm's Contingency Plan

Plan Rating	Nonexistent	Poor	Okay	Good	Excellent
Preparedness	Backup only	Own a backup server	Co-located facility where systems reside	Ability to restore systems manually on a regular basis	Automated synchronization or equivalent on a daily basis
Philosophy	"I can't imagine I'd ever need to, but I'm confident that everything will be restored with the tape."	"I assume my IT folks will drop everything else to get my firm going again if there is a disaster."	"I've established a site to house my equipment and realize that I still need to have a more robust plan."	"I realize that it's going to take time to restore my data, but I'm prepared to make do without all of my systems for a couple of business days."	"My firm made a substantial investment to ensure that my systems are up and running ASAP, but I know the switch will take time to implement."
Recovery Time	1-2 weeks	1 week	3-4 days	1-2 days	2-4 hours
Stage	Denial	Acceptance	Planning	Implementing	Validation
Cost	$	$$	$$$	$$$$	$$$$$

SERVICE CONTINUITY MANAGEMENT

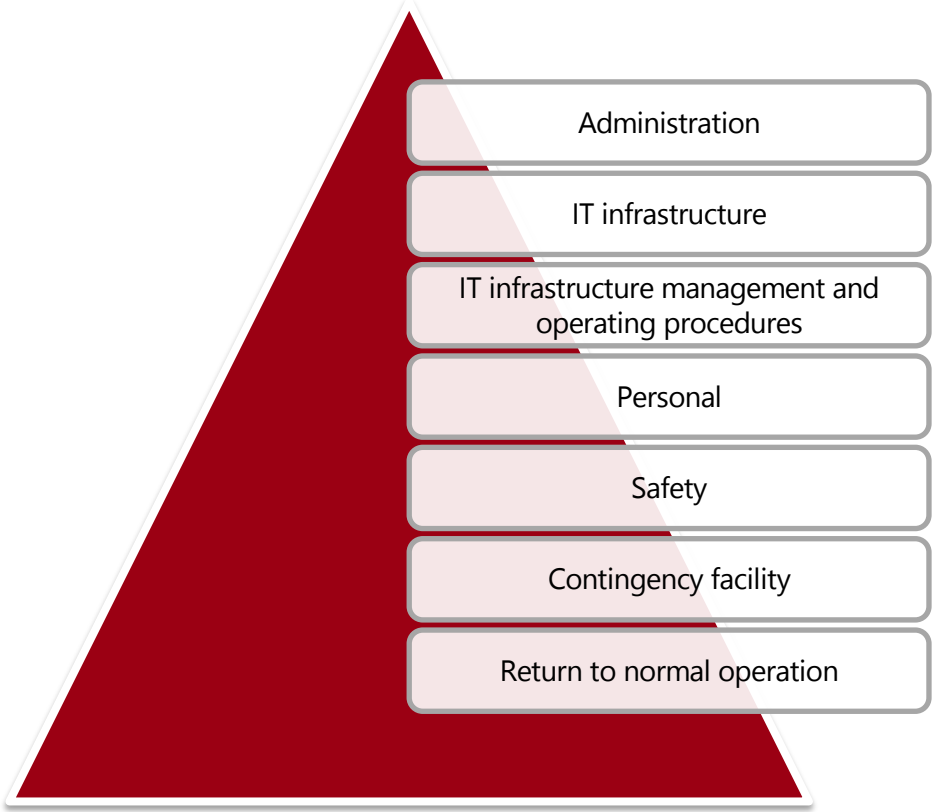
Service continuity
is a set of clearly defined plans related to how an organization will recover from a disaster and return to a pre-disaster condition, considering the four dimensions of service management

Service continuity plans usually include:
- Response plan
- Recovery plan
- Plan of returning to normal operations

Business continuity plans may include:
- emergency response to interface with all emergency services and activities
- evacuation plan to ensure the safety of personnel
- crisis management and public relations plan plans for the command and control of different crises and the management of the media and public relations
- security plan showing how all aspects of security will be managed on all home sites and recovery sites
- communication plan showing how all aspects of communication will be handled and managed with all relevant areas and parties involved during a major incident

Contingency Plan

the 7 sections of the plan

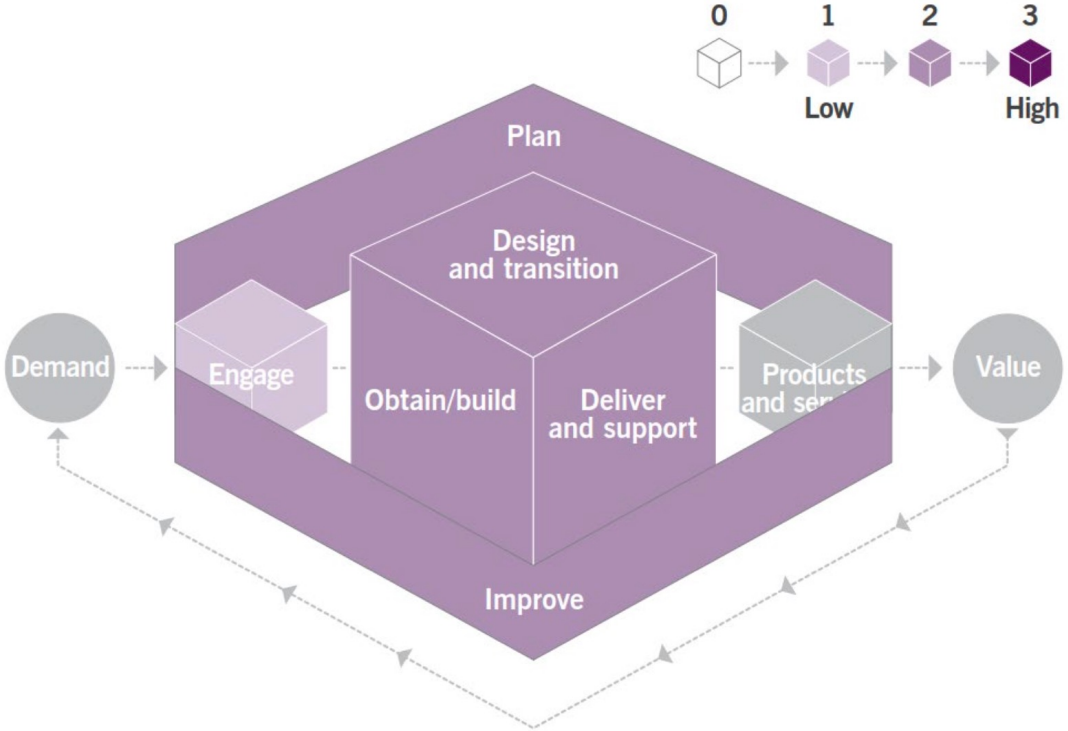


Contingency Plan: an example

SAMPLE EVENT

CONTINGENCY PLAN

ITEM	WHAT CAN GO WRONG	SEVERI
Keynote Speaker	No-show	High
Wi-Fi	Doesn't work	Medium
Catering	Food isn't delivered	High
Registration desk	Registration sheets go missing	Low



Heat map of the contribution of service continuity management to value chain activities

What is the purpose of the 'change control' practice?

- Supporting the agreed quality of a service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner
- Making new and changed services and features available for use
- Ensuring that risks are properly assessed, authorizing changes to proceed and managing a change schedule in order to maximize the number of successful IT changes
- Aligning an organization's practices and services with changing business needs through the ongoing identification and improvement of all elements involved in the effective management of products and services

Identify the missing word(s) in the following sentence. A known error is a(n) [?] that has been analyzed but has not been resolved.

- Change
- Incident
- Event
- Problem

Which practice provides a single point of contact for users?

- Change control
- Incident management
- Service request management
- Service Desk