

ITIL – Introducing service transition

The goals of service transition

“Aligning the new or changed service with the organisational requirements and organisational operations”

- Plan and manage the capacity and resources required to package, build, test and deploy a release into production
- Provide a consistent and rigorous framework for evaluating the service capability and risk profile before a new or changed service is released
- Establish and maintain the integrity of all identified service assets and configurations
- Provide good quality knowledge and information to expedite effective decisions about promoting a release
- Provide efficient, repeatable build and installation mechanisms to deploy releases to test and production
- Ensure that the service can be managed, operated and supported in accordance with service design

Other objectives include:

- Align the new or changed service with the organisation requirements and business operations
- Ensure that customers/users can use the new or changed service in a way that maximises value to the organisation operations
- Plan and manage resources so that transitions come in on time, cost and quality
- Ensure minimum impact on current services
- Increase customer, user and service support satisfaction

Value to the organisation/business of service transition

Creates value for the business by improving:

- The ability to adapt quickly to new requirements
- The success rate of changes and releases for the organisation
- The predictions of service levels and warranties for new and changed services
- Confidence in the degree of compliance with the organisation requirements during change
- Clarity of plans so the business can link their organisation change plans to transition plans

All the above give *competitive edge* and help the agility and flexibility and the organisation.

The scope of service transition

The scope of service transition includes the management and coordination of the processes, systems and functions to package, build, test and deploy a release into production and establish the service specified in the customer and stakeholder requirements.

The following activities are excluded from the scope of service transition best practices:

- Minor modifications to the production services and environment, for example, replacement of a failed PC or printer, installation of standard software on a PC or server, new user
- Ongoing continual service improvements that do not significantly impact the services or service provider’s capability to deliver the services, for example, request fulfilment activities driven from service operations

Service transition processes

- Knowledge management
- Change management
- Release and deployment management
- IT service asset and configuration management
- Service validation and testing

Knowledge management

Why have knowledge management?

An organisations ability to deliver a quality service or process rests, to a significant extent, on its ability to respond to circumstances. To enable this to happen, those involved must have a sound understanding of the situation, the options, consequences and benefits. An example of this knowledge in the service transition phase may include:

- Identity of stakeholders
- Acceptable risk levels and performance expectations
- Available resource and timescales

The quality and relevance of the knowledge rests in turn on the accessibility, quality and continued relevance of the underpinning data and information available to service staff.

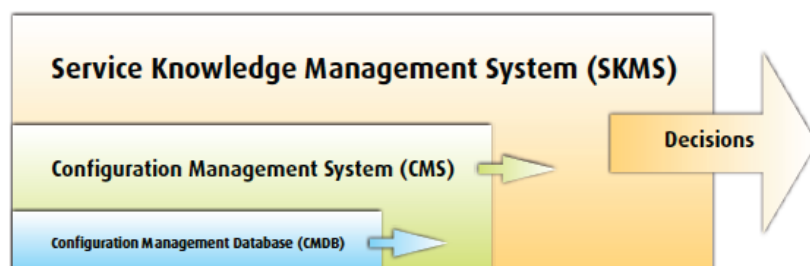
The objectives of knowledge management

“The goal of knowledge management is to enable organisations to improve the quality of management decision-making by ensuring that reliable and secure information and data is available throughout the service lifecycle”

The primary purpose is to improve efficiency by reducing the need to rediscover knowledge.

This is achieved by:

- Enabling the service provider to be more efficient and improve the quality of the service, reduce costs, increase satisfaction
- Ensuring staff have a clear and shared understanding of the value that their services provide to customers and how they are realised
- Ensuring that, as required, service provider staff have adequate information on –
 - Who is currently using the service they are providing
 - The current states of consumption
 - Service delivery constraints
 - Difficulties faced by customers, realising the expected benefits from services



The above diagram is a very simplified illustration of the relationship of the three levels, with data being gathered within the CMDB, and feeding through the CMS into the SKMS as information to support the informed decision making process.

Value to the organisation of knowledge management

Knowledge management is especially significant within service transition since relevant and appropriate knowledge is one of the key service elements being transitioned. Examples where successful transition rests on appropriate knowledge management include:

- User, service desk, support staff and supplier understanding of the new or changed service, including knowledge of errors signed off before deployment, to facilitate their roles within that service
- Awareness of the use of the service, and the discontinuation of previous versions
- Establishment of the acceptable risk and confidence levels associated with the transition, e.g. measuring, understanding and acting correctly on results of testing and other assurance results

Effective knowledge management is a powerful asset for people in all roles across all stages of the service lifecycle. It is an excellent method for individuals and teams to share data, information and knowledge about all facets of an IT service. The creation of a single system for knowledge management is recommended.

The activities of knowledge management

Knowledge identification capture and maintenance – Specifically knowledge management will identify and plan for the capture of relevant knowledge and the consequential information and data that will support it.

Knowledge transfer – This is the activity through which one unit (e.g. group or department) is affected by the experiences of another. The form of knowledge transfer must suit those who will use it, examples of criteria/examples that can be used are:

- Learning styles
- Knowledge visualisation
- Driving behaviour
- Seminars, webinars and advertising
- Journals and newsletters

The transfer of knowledge can be observed through changes in the knowledge or performance or recipients, and at an individual or unit level.

Data and information management – Knowledge rests on the management of the information and data that underpins it. For this process to be efficient it requires answers to some key input questions, such as how the data and information will be used, what conditions will need to be monitored, what data is available, what are the associated costs, legislative and requirements etc.

Establishing data and information requirements – Often, data and information is collected with no clear understanding of how it will be used and this can be costly. Efficiency and effectiveness are delivered by establishing the requirements for information.

Establishing data and information management procedures – When the requirements have been set up, data and information management to support knowledge management can be established. This will include, defining procedures required to maintain the data and information, procedures for access, storage (including backup and recovery), retrieval, rights and responsibilities etc.

Evaluation and improvement – As with all processes, the capture and use of data and information to support knowledge management and decision making requires attention to ongoing improvement.

The service improvement plan, produced by the Service Level Manager, will use the following relevant input:

- Measurements of the use made of the data transactions
- Evaluate usefulness of the data and information
- Identification of any data or information (or registered users) that is no longer to the organisation's knowledge requirements

The terminology of knowledge management

SKMS: Service knowledge management System

CMS: Configuration Management System

KEDB: Known Error Database

DML: Definitive Media Library. The secure library in which the definitive authorised versions of all media CIs are stored and protected. The DML should include definitive copies of purchased software (along with license documents or information), as well as software developed on site

Change management

Why have change management?

Change is inevitable, and the rate of change in technology is increasing and the organisation's processes and business models constantly have to adapt to the economic climate, competitive pressures, and the opportunity to create through change and innovation. Change management, as a discipline in distributed computing is usually somewhat lacking. Yet, change management for IT operations is critical to improving availability, performance and throughput. Strong operational change management reduces errors, as well as planned and unplanned downtime.

Changes arise for a variety of reasons:

- Proactively, e.g. seeking organisational benefits such as reducing costs or improving services or increasing the ease and effectiveness of support
- Reactively as a means of resolving errors and adapting to changing circumstances

Changes should be managed to:

- Optimise risk exposure (supporting the risk profile required by the organisation)
- Minimise the severity of any impact and disruption
- Be successful at the first attempt

Such an approach will deliver direct financial benefit for the organisation by delivering early realisation of benefits (or removal of risk), with a saving of money and time.

To make an appropriate response to all requests for change entails a considered approach to assessment of risk and business continuity, change impact, resource requirements, change authorisation and especially to the realisable organisation benefit. This considered approach is essential to maintain the required balance between the need for change and the impact of the change.

The objectives of change management

The goal of the change management process is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of change related Incidents upon service quality, and consequently to improve the day to day operations of the organisation.

Other objectives include:

- Respond to changing business requirements
- Minimise impact/risk of implementing changes
- Ensure all changes are approved at the appropriate level with the business and IT
- Implement changes successfully
- Implement changes in times that meet business needs
- Use standard processes to record all changes

Not every change is an improvement, but every improvement is a change!

The scope of change management

Addition, modification or removal of:

- Any service or configuration Item or associated documentation

Including

- Strategic, tactical and operational changes

Excluding

- Business strategy and process
- Anything documented as out of scope

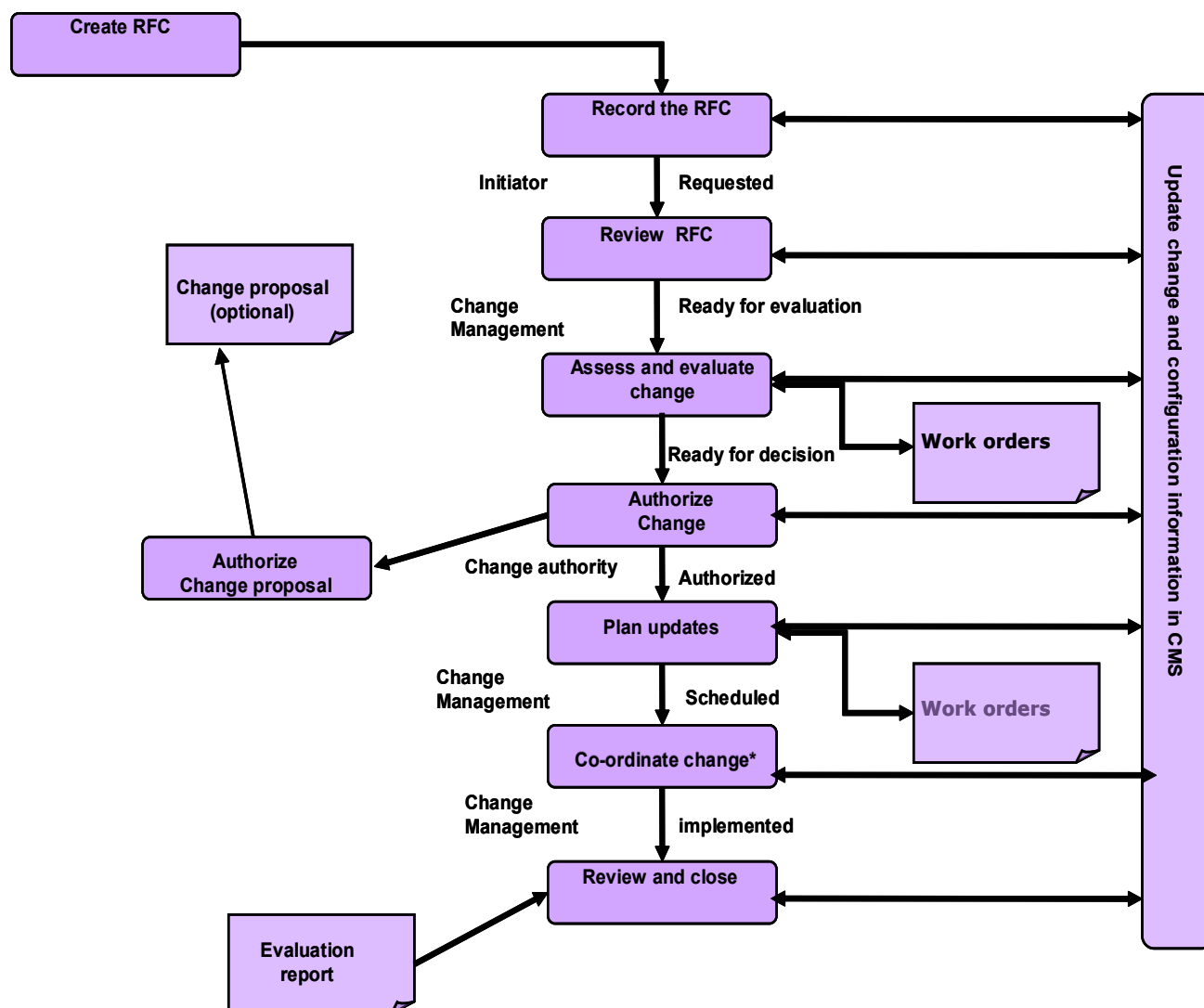
The activities of change management

Activities undertaken will involve:

- Change logging and filtering/acceptance
 - Does the RFC (request for change) have enough, quality, information
 - Unique identification number
 - Filter out impractical RFCs and provide feedback to issuer
- Managing changes and the change process
 - Prioritise RFCs (based on risk assessment)
 - Categorise RFCs (e.g. minor, significant or major impact)
- Chairing the CAB (Change Advisory Board) and the ECAB (Emergency Change Advisory Board)
 - Assess all RFCs (but not all during the meeting!! CAB is a consulting body)
 - Impact and resource assessment
 - Approval based on financial, business and technical criteria
 - The Forward Schedule of Change (FSC)
- Coordinate the change
 - Supported by release management, change management coordinates the building, testing and implementation of the change
- Reviewing and closing RFCs
- Management reporting

Emergency changes follow the same steps, but usually in a different order. The ECAB approves an emergency change immediately and the building, testing and implementation are done before the paperwork, which is usually completed retrospectively, but don't forget the documentation!

The change process



The value to the organisation of change management

- Prioritising and responding to organisation and customer/user change proposals
- Implementing changes that meet the customers' agreed service requirements while optimising costs
- Contributing to meet governance, legal, contractual and regulatory requirements
- Reducing failed changes and therefore service disruption, defects and rework
- Delivering change promptly to meet business timescales
- Tracking changes through the service lifecycle
- Contributing to better estimations of the quality, time and cost of change
- Assessing the risks associated with the transition of services
- Aiding productivity of staff through minimising disruptions due to high levels of unplanned or *emergency* change and hence maximising service availability
- Reducing the Mean Time to Restore Service (MTRS), via quicker and more successful implementations of corrective changes

The terminology of change management

Normal change

A change that follows all of the steps of the change process.

Standard change

A pre-approved change that is low risk, relatively common and follows a procedure or work instruction, e.g. password reset or provision of standard equipment to a new employee. RFC's are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request.

Emergency change

A change that must be introduced as soon as possible. e.g. to resolve a major incident or implement a security patch. The change management process will normally have a specific procedure for handling emergency changes.

Requests for change

Every change to the IT Infrastructure has to go through change management. A Request for Change (RFC) is formally issued for every change request.

The Change Manager

Responsible for the change management process.

Change Advisory Board (CAB)

A dynamic group of people (depending on the change) that approve changes with medium to high priority, risk and impact.

CAB/EC

CAB Emergency Committee approves and authorises changes with high urgency, risk and impact.

Change models

Some organisations use change models prior to implementation to estimate the impact of the change. Change management and capacity management work together on this.

FSC

The Forward Schedule of Change (FSC) contains details of all approved changes and their proposed implementation date.

Release and deployment management

Why have release and deployment management

The goal of release and deployment management is to deploy releases into production and enable effective use of the service in order to deliver value to the organisation/customer/user.

The objectives of release and deployment management

The objective of release and deployment management is to build, test and deliver the capability to provide the services specified by service design. This includes the processes, systems and functions to package, build, test and deploy a release into production and prepare for service operation.

Other objectives include:

- To provide clear and comprehensive plans enabling change projects to align their activities
- To ensure that the hardware and software being changed is traceable, secure and that only correct, authorised and tested versions are installed
- To ensure that master copies of all software are secured in the Definitive Media Library (DML)
- To ensure that release packages are built, installed, tested and deployed efficiently
- To ensure that skills and knowledge are transferred to operations and support staff
- To ensure that new or changed services meet the utility, warranty and service levels

- Minimise unpredicted impact
- To communicate and manage expectations of the customer during the planning and rollout of new releases

The scope of release and deployment management

The scope of release and deployment management includes the processes, systems and functions to package, build, and test and deploy a release into production and establish the service specified in the service design package before final handover to service operations.

The value to the organisation of release and deployment management

Effective release and deployment management enables the service provider to add value to the organisation by:

- Delivering change, faster and at optimum cost and minimised risk
- Assuring that customers and users can use the new or changed service in a way that supports the organisation goals
- Improving consistency in implementation approach across the organisation change, service teams, suppliers and customers

Release and deployment management activities

- Release policy and planning
- Release design, build and configuration
- Release testing and acceptance
- Deployment and planning
- Extensive testing to predefined acceptance criteria
- Sign off of the release for implementation
- Communication, preparation and training
- Audits of hardware and software prior to and following the implementation of changes
- Installation of new or upgraded hardware
- Storage of controlled software in both centralised and distributed systems
- Release, deployment and the installation of software

Release units

A *release unit* describes the portion of a service or IT infrastructure that is normally released together according to the organisation's release policy. The unit may vary, depending on the type(s) or item(s) of service asset or service component, such as software and hardware.

The objective is to decide the most appropriate release unit level for each service asset or component. An organisation may, for example, decide that the release unit for critical applications is the complete application in order to ensure that testing is comprehensive. The same organisation may decide that a more appropriate release unit for a website is at the page level.

The following factors should be taken into account when deciding the appropriate level for release units:

- The ease and amount of change necessary to release and deploy a release unit
- The amount of resources and time needed to build, test, distribute and implement a release unit
- The complexity of interfaces between the proposed unit and the rest of the services and IT infrastructure

Release and deployment options

Big bang – The new or changed service is deployed to all user areas in one operation. This will often be used when introducing an application change and consistency of service across the organisation is considered important.

Phased – The service is deployed to a part of the user base initially, and then this operation is repeated for subsequent parts of the user base via a scheduled rollout plan.

Push – Is used where the service component is deployed from the centre and pushed out to the target locations.

Pull – Used for software releases, where the software is made available in a central location, but users are free to pull the software down to their own location at a time of their choosing or when a workstation restarts.

Automation – Helps to ensure repeatability and consistency. The time required to provide a well designed and efficient automated mechanism may not always be available or viable.

Manual – Important to monitor and measure the impact of many repeated manual activities, as they are likely to be inefficient and error prone.

The terminology of release and deployment management

Release – A collection of authorised changes to an IT service.

Release unit – The portion of the IT infrastructure that is released together, e.g. major release: major roll out of new hardware and/or software; minor release: a few minor improvements and fixes to known errors. Emergency fix: a temporary or permanent quick fix for a problem or known error.

Definitive Spares (DS) – (previously known as DHS) Physical storage of all spare IT components and assemblies maintained at the same level as within the live environment. These can then be used when needed for additional systems or in the recovery from incidents (details are recorded in the CMDB, controlled by release management).

Definitive Media Library (DML) – (previously known as the DSL) the secure library in which the definitive authorised versions of all media CIs are stored and protected. The DML should include definitive copies of purchased software (along with license documents or information) as well as software developed on site.

CMDB – Configuration Management Database.

Service asset and configuration management

Why have service asset and configuration management

This process ensures the integrity of service assets and configurations in order to support the effective and efficient management of the IT organisation.

The main reason for configuration management is to gather the information needed (in a non-duplicated manner) about the IT components and how they relate to each other. The reason for this is to ensure that the relevant information is available for all the other processes to ensure that detailed impact and risk analysis can take place.

The objectives of service asset and configuration management

- Account for all the IT assets and configurations within the organisation and its services
- Provide accurate information on configurations and their documentation to support all the other service management processes
- Provide a sound basis for incident management, problem management, change management and release management
- Verify the configuration records against the infrastructure and correct any exceptions
- Plan, identify, control, record, report, audit and verify service assets and configuration items
- Account for manage and protect the integrity of service assets and configuration items throughout their lifecycle
- Provide accurate information to support business and service management
- Ensure the integrity of those items by creating and maintaining an accurate Configuration Management System (CMS) as part of the Service knowledge management System (SKMS)

The value to the organisation of service asset and configuration management

Optimising the performance of service assets and configurations improves the overall service performance and optimises the costs and risks caused by poorly managed assets, e.g. service outages, fines, correct licence fees and failed audits. SACM provides visibility of accurate representations of a service, release or environment that enables:

- Better forecasting and planning of changes
- Changes and releases to be assessed, planned and delivered successfully
- Incidents and problems to be resolved within the service level targets
- Service levels and warranties to be delivered
- Better adherence to standards, legal and regulatory obligations
- More business opportunities as able to demonstrate control of assets and services
- Changes to be traceable from requirements

The activities of service assets and configuration management

Configuration management planning

A configuration management plan should define:

- The purpose, scope and objectives of configuration management
- Related policies, standards and processes that are specific to the support group
- Configuration Management roles and responsibilities
- CI (Configuration Item) naming conventions
- The schedule and procedures for performing Configuration Management activities: configuration identification, control, status accounting, configuration audit and verification
- Interface control with third parties, e.g. Change Management, suppliers
- Configuration management systems design, including scope and key interfaces

Configuration identification

- CIs are the components used to deliver a service. The CIs include software, documentation and SLA's
- Also identify the relationship between CI's and the attributes for every CI

Control of CI's

The objective of configuration control is to ensure that only authorized and identifiable CI's are recorded in the CMDB upon receipt.

Configuration status accounting

- Status reports should be produced on a regular basis, listing, for all CI's under control, their current version and change history. Status accounting reports on the current, previous and planned states of the CI's should include:
 - Unique identifiers of constituent CI's and their current status, e.g. *under development*, *under test*, *live*
 - Configuration baselines, releases and their status
 - Latest software item versions and their status for a system baseline/application
 - The person responsible for status change, e.g. from *under test* to *live*
 - Change history/audit trail
 - Open problems/RFC's

Configuration verification and audit

- Service desk staff, while registering incidents, can do daily verification
- Configuration audits should be considered at the following times:
 - Shortly after implementation of a new configuration management system
 - Before and after major changes to the IT infrastructure
 - Before a software release or installation to ensure that the environment is as expected
 - Following recovery from disasters and after a *return to normal* (this audit should be included in contingency plans)

At random intervals

- In response to the detection of any unauthorised CI's
- At regular intervals

Configuration Management Database (CMDB)

- Backup, administration, housekeeping

Service validation and testing

Why have service validation and testing?

The goal of service validation and testing is to assure that a service will provide value to organisation.

The underlying concept to which service validation contributes is quality assurance – establishing that the service design and release will deliver a new or changed service or service offering that is fit for the purpose and fit for use. Testing is a vital area within service management and has often been the unseen underlying cause of what was taken to be inefficient service management processes.

If services are not tested sufficiently then their introduction into the operational environment will bring rise in:

- Incidents – failures in service elements and mismatches between what was wanted and what was delivered impact on business support
- Service desk calls for assistance – services that are not functioning as intended are inherently less intuitive causing higher support requirements
- Problems and errors – that are harder to diagnose in the live environment
- Costs – since errors are more expensive to fix in production than if found in testing
- Services – that are not used effectively by the users to deliver the desired value

The objectives of service validation and testing

The objectives are:

- Provide confidence that a release will create a new or changed service or service offerings that deliver the expected outcomes and value for the customers within the projected costs, capacity and constraints
- Validate that a service is *fit for purpose* – it will deliver the required performance with desired constraints removed
- Assure a service is *fit for use* – it meets certain specifications under the specified terms and conditions of use
- Confirm that the customer and stakeholder requirements for the new or changed service are correctly defined, and remedy any errors or variances early in the service lifecycle as this is considerably cheaper than fixing errors in production

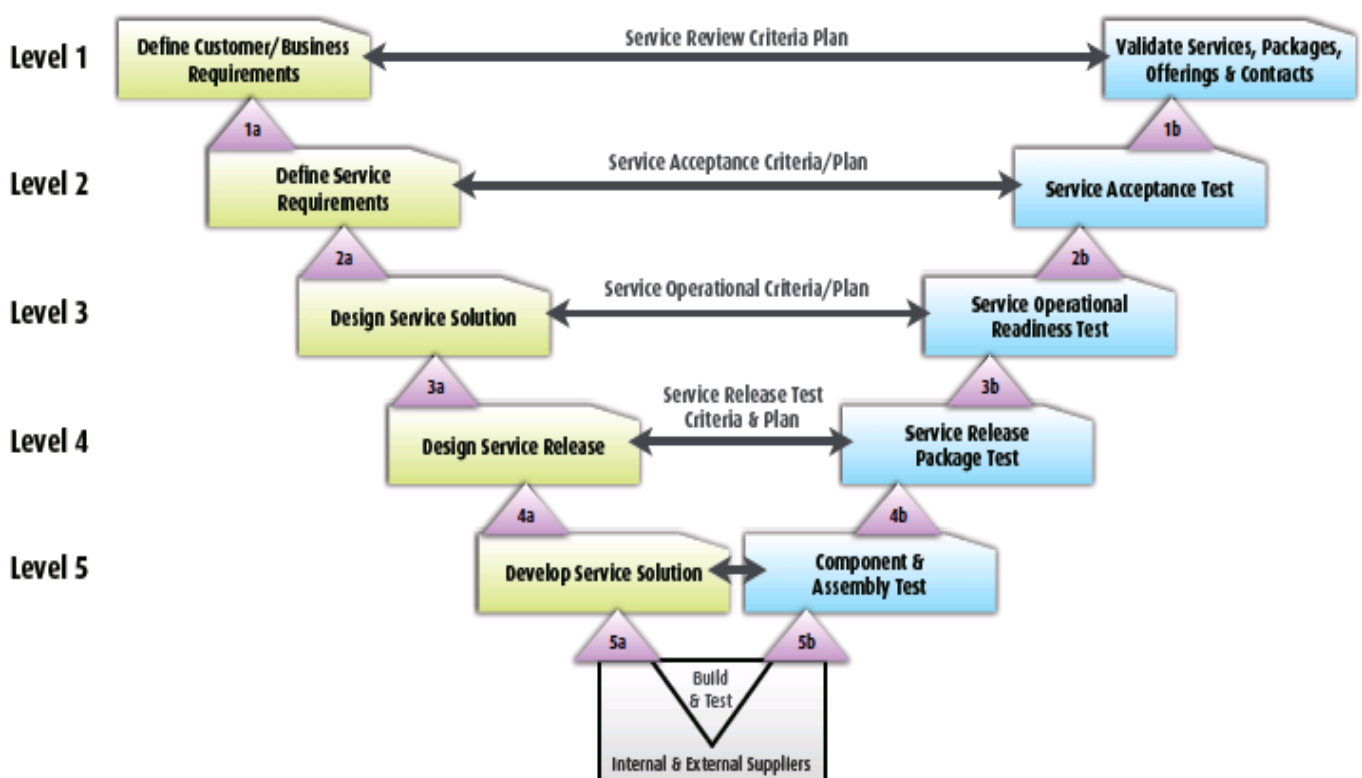
The value to the organisation of service validation and testing

Service failures can harm the organisation and can result in outcomes such as:

- loss of reputation
- loss of money
- loss of time

The key value to the business and customers from service testing and validation is in terms of the established degree of confidence that a new or changed service will deliver the value and outcomes required of it and understanding the risks. Successful testing depends on all parties understanding that it cannot give, indeed should not give, any guarantees but provides a measured degree of confidence. The required degree of confidence varies depending on the customer's business requirements and pressures of an organisation.

The V model



The V Model concept of establishing acceptance requirements against the requirements and design can apply, with each iterative design being considered for the degree of integrity and competence that would **justify release to the customer for trial and assessment**.

The **left hand** side represents the specification of the service requirements down to the detailed service design.

The **right hand** side focuses on the validation and test activities that are performed against the specifications defined on the left hand side, there is direct involvement by the equivalent party on the right hand side.

It shows that service validation and acceptance test planning should start with the definition of service requirements, e.g. customers who sign off the agreed service requirements will also sign off the service acceptance criteria and test plan.

The terminology of service validation and testing

Validation

The 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 phase.

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.

Test

The activity that verifies that a CI, IT service, process etc., meets its specification or agreed requirements.

Evaluation

Responsible for assessing a new or changes IT service to ensure that risks have been managed and to help determine whether to proceed with the change.

Fit for purpose

Describes whether the process, CI, IT service etc., is capable of meeting its objectives or service levels.

Fit for use

Meets certain specifications under the specified terms and conditions of use.