ITIL® Lifecycle Service Transition

ITILKONSULTEN
KATOKITSU UTBILDNING

Arrangements

Contents

Times:

1st day: 9 - 17
2nd day: 9 - 17
3rd day: 9 – 16
4th day: 9 - 16

Lunch: 12 – 13

Service Transition Life cycle

The guidance focuses on how to ensure that the requirements from service strategy, developed in service design, are effectively realized in service operation while controlling the risks of failure and subsequent disruption.

Purpose

The purpose of the service transition stage of the service lifecycle is to ensure that new, modified or retired services meet the expectations of the business as documented in the service strategy and service design stages of the lifecycle.

Objectives

The objectives of service transition are to:

- Plan and manage service changes efficiently and effectively
- Manage risks relating to new, changed or retired services
- Successfully deploy service releases into supported environments
- Set correct expectations on the performance and use of new or changed services
- Ensure that service changes create the expected business value
- Provide good-quality knowledge and information about services and service assets.

Scope

- Managing the complexity associated with changes to services and service management processes
- Allowing for innovation while minimizing the unintended consequences of change
- Introducing new services
- Changes to existing services, e.g. expansion, reduction, change of supplier, acquisition or disposal of sections of user base or suppliers, change of requirements or skills availability
- Decommissioning and discontinuation of services, applications or other service Components
- Transferring services to and from other service providers.

Value to business

- Enable projects to estimate the cost, timing, resource requirement and risks associated with the service transition stage more accurately
- Result in higher volumes of successful change
- Enable service transition assets to be shared and re-used across projects and services
- Reduce delays from unexpected clashes and dependencies – for example, if multiple projects need to use the same test environment at the same time

Value to business, cont

$ Reduce the effort spent on managing the service transition test and pilot environments

$ Improve expectation setting for all stakeholders involved in service transition including customers, users, suppliers, partners and projects

$ Increase confidence that the new or changed service can be delivered to specification without unexpectedly affecting other services or stakeholders

$ Ensure that new or changed services will be maintainable and cost-effective

$ Improve control of service assets and configurations.

Policies

Policies

Context

A formal policy for service transition should be defined, documented and approved by the management team, who ensure that it is communicated throughout the organization and to all relevant suppliers and partners.

- Define and implement a formal policy for service transition
- Implement all changes to services through service transition
- Adopt a common framework and standards
- Maximize re-use of established processes and systems
- Align service transition plans with the business needs
- Establish and maintain relationships with stakeholders
- Establish effective controls and disciplines
- Provide systems for knowledge transfer and decision support
- Plan release packages
- Anticipate and manage course corrections
- Proactively manage resources across service transitions
- Ensure early involvement in the service lifecycle
- Provide assurance of the quality of the new or changed service
- Proactively improve quality during service transition.

Policies, cont

- Policies should clearly state the objectives, and any non-compliance with the policy must be remedied.
- Policies should be aligned with the overall governance framework, organization and service management policies, with appropriate auditing and enforcement. This should include alignment with ISO/IEC 20000, ISO/IEC 38500 and COBIT where these have been adopted.
- Sponsors and decision makers involved in developing the policy must demonstrate their commitment to adapting and implementing the policy. This includes the commitment to deliver predicted outcomes from any change in the services.
- Processes should integrate teams, blending competencies while maintaining clear lines of accountability and responsibility.
- Changes should be delivered in releases, except for standard changes and some emergency changes.
- Deployment must be addressed early in the release design and release planning stages.

Purpose	Objectives	Scope	Value to business	Policies

Context

Context

Context

•Portfolio Mgt •Demand Mgt •Financial Mgt •Business Relationship Mgt	•Supplier Mgt •Information Security Mgt •Service Catalogue Mgt •Service Level Mgt •IT Service Continuity Mgt •Availability Mgt •Capacity Mgt •Design Coordination •. . .	•Transition Planning and Support •Change Mgt •Service Asset and Configuration Mgt •Release and Deployment Mgt •Service Validation and Testing •Knowledge Mgt	•Incident Mgt •Problem Mgt •Event Mgt •Access Mgt •Request fullfilment

Service Strategy → Service Design → Service Transition → Service Operation

Continual Service Improvement

Service Transition processes

The transition processes are considered from the management perspective:

i.e., those aspects that are required to

- understand and control each process and its interfaces,
- oversee the implementation and ongoing improvement of, and compliance to each process,
- judge the effectiveness and efficiency of each process.

Purpose

Transition Planning and Support

Purpose

The purpose of the transition planning and support process is to provide overall planning for service transitions and to coordinate the resources that they require.

Transition Planning and Support

Objectives

Plan and coordinate the resources to ensure that the requirements of service strategy encoded in service design are effectively realized in service operation.

Coordinate activities across projects, suppliers and service teams where required.

Establish new or changed services into supported environments within the predicted cost, quality and time estimates.

Establish new or modified management information systems and tools, technology and management architectures, service management processes, and measurement methods and metrics to meet requirements established during the service design stage of the lifecycle.

Transition Planning and Support

Objectives, cont

Ensure that all parties adopt the common framework of standard re-usable processes and supporting systems in order to improve the effectiveness and efficiency of the integrated planning and coordination activities.

Provide clear and comprehensive plans that enable customer and business change projects to align their activities with the service transition plans.

Identify, manage and control risks, to minimize the chance of failure and disruption across transition activities; and ensure that service transition issues, risks and deviations are reported to the appropriate stakeholders and decision makers.

Monitor and improve the performance of the service transition lifecycle stage.

Transition Planning and Support

Principles and basic concept

The service transition planning and support process incorporates the service design and operational requirements within the transition planning.
This involves the management and control of the transition plan, specifically the coordination of the following aspects:

- Integration and alignment of the transition planning with the customer, service and contract portfolio.
- Coordination of the progress of the transition with modifications, pending items, risks and variances.
- Quality review of all service transition, release and deployment plans.
- Implementation of the transition process, support systems and tools.
- Monitoring and improvement of the service transition performance.

Transition Planning and Support

Policy

Transition Planning and Support is mainly based on the policies defined for the whole lifecycle.

Also, each and every process defined in the Service Transition lifecycle has a detailed, process specific policy, e.g. Change Management, Release and Deployment Managment, Etc.

Transition Planning and Support

Strategy approach

- Transition model including service transition lifecycle stages
- Plans for managing changes, assets, configurations and knowledge
- Baseline and evaluation points
- Configuration audit and verification points
- Points where change authorization is needed
- Use of change windows
- Transition estimation, resource and cost planning
- Change evaluation and change authorization
- Release planning, build, test, deployment and early life support
- Error handling, correction and control
- Management and control – recording, progress monitoring and reporting
- Service performance and measurement system
- Key performance indicators (KPIs) and improvement targets

Transition Planning and Support

Scope

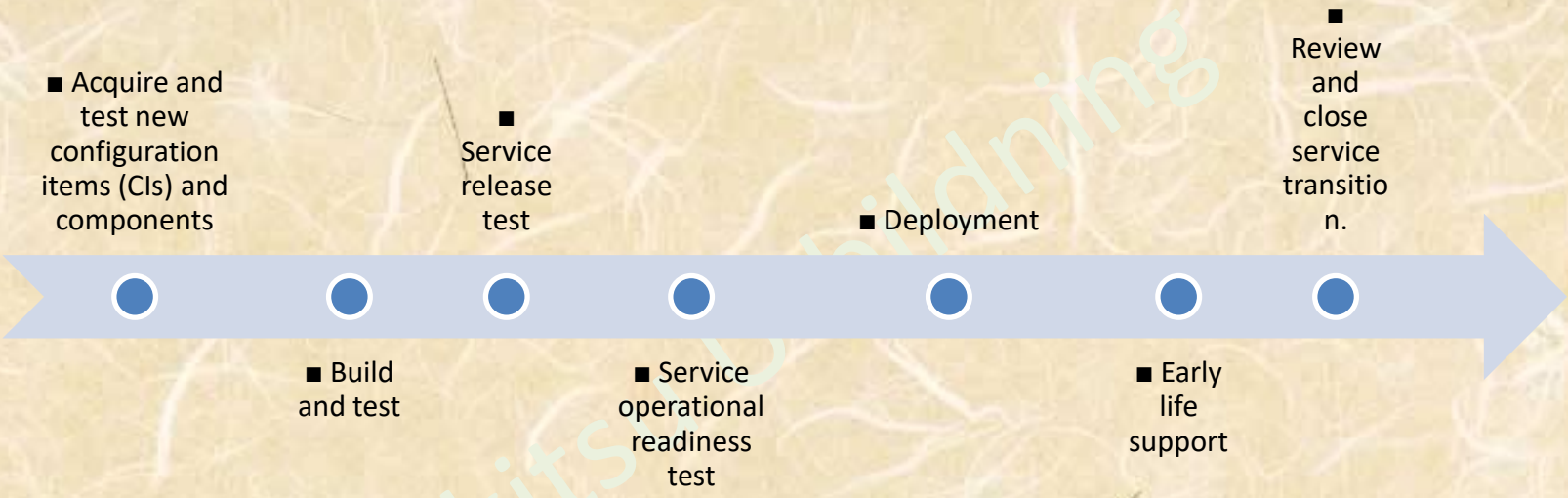
- Maintaining policies, standards and models for service transition activities and processes
- Guiding each major change or new service through all the service transition processes
- Coordinating the efforts needed to enable multiple transitions to be managed at the same time
- Prioritizing conflicting requirements for service transition resources
- Planning the budget and resources needed to fulfil future requirements for service transition
- Reviewing and improving the performance of transition planning and support activities
- Ensuring that service transition is coordinated with programme and project management, service design and service development activities.

Transition planning and support *is not responsible* for detailed planning of the build, test and deployment of individual changes or releases;

these activities are carried out as part of change management and release and deployment management.

Transition Planning and Support

Stages

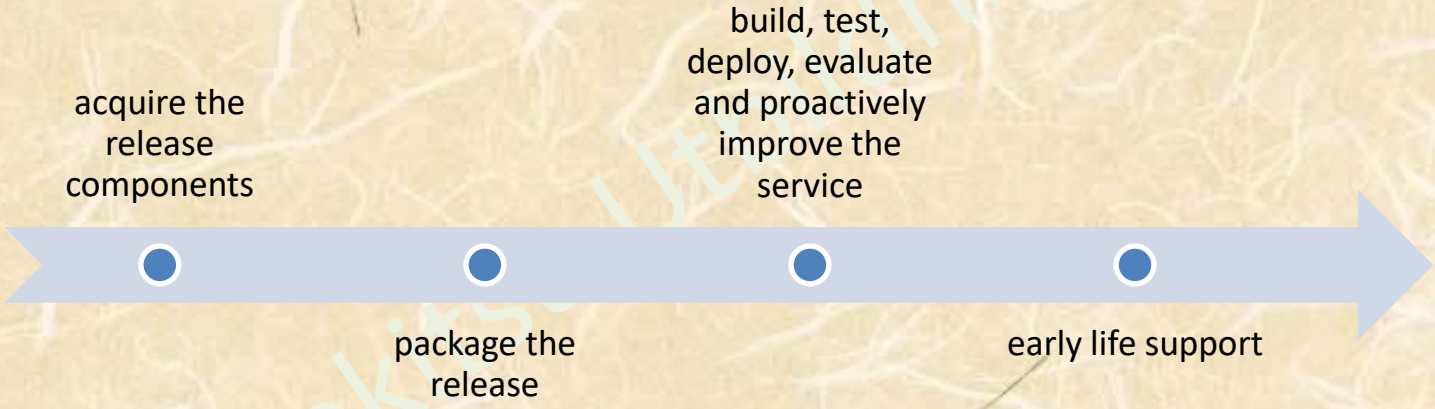


For each stage there will be exit and entry criteria and a list of mandatory deliverables from the stage. These criteria are often implemented as ‘quality gates’ at specific stages in the *design and transition* of a new or changed service.

Transition Planning and Support

Milestones

An overarching service transition plan should include the milestone activities to



It will also include the activities to build and maintain the services and IT infrastructure, systems and environments and the measurement system to support the transition activities.

Transition Planning and Support

Metrics

- Cost of testing and evaluation versus cost of live incidents
- Delays caused by service transition, e.g. due to a lack of service transition resources
- Operational problems that could have been identified by the service transition processes

Transition Planning and Support

Main Inputs and Outputs

The main input to service transition is a *service design package*, which includes all of the information needed to manage the entire lifecycle of a new or changed service.

The main output is the *deployment into live use* of a new or changed service, with all the supporting knowledge and information, tools and processes required to support the service.

Transition Planning and Support

Service strategy input / output

Service Strategy	Vision and mission Service portfolio Policies Strategies and strategic plans Priorities Change proposals, including utility and warranty requirements and expected timescales Financial information and budgets Input to change	Transitioned services Information and feedback for business cases and service portfolio Response to change proposals Service portfolio updates Change schedule Feedback on strategies and policies Financial information for input to budgets Financial reports Knowledge and information in the SKMS

Transition Planning and Support

Service Design input / output

	Inputs	Outputs
Service Design	Service catalogue Service design packages, including: ■ Details of utility and warranty ■ Acceptance criteria ■ Service models ■ Designs and interface specifications ■ Transition plans ■ Operation plans and procedures ■ Requests for change (RFCs) to transition or deploy new or changed services ■ Input to change evaluation and CAB meetings ■ Designs for service transition processes and procedures ■ Service level agreements, operational level agreements and underpinning contracts	■ Service catalogue updates ■ Feedback on all aspects of service design and service design packages ■ Input and feedback on transition plans ■ Response to RFCs ■ Knowledge and information in the SKMS (including the CMS) ■ Design errors identified in transition for redesign ■ Evaluation reports

Transition Planning and Support

Service Operations input / output

	Inputs	Outputs
Service Operation	■ RFCs to resolve operational issues ■ Feedback on quality of transition activities ■ Input to operational testing ■ Actual performance information ■ Input to change evaluation and CAB meetings	■ New or changed services ■ Known errors ■ Standard changes for use in request fulfilment ■ Knowledge and information in the SKMS (including the CMS)

Transition Planning and Support

Continual Service Improvement /CSI)

	Inputs	Outputs
CSI	■ Results of customer and user satisfaction surveys ■ Input to testing requirements ■ Data required for metrics, key performance indicators (KPIs) and critical success factors (CSFs) ■ Input to change evaluation and CAB meetings ■ Service reports ■ RFCs for implementing improvements	■ Test reports ■ Change evaluation reports ■ Knowledge and information in the SKMS ■ Achievements against metrics, KPIs and CSFs ■ Improvement opportunities logged in the continual service improvement register

After planning – before transition start

Before starting the release, the service transition planning role should verify the plans and ask appropriate questions such as:

- ✓ Are the service transition and release plans up to date?
- ✓ *Have the plans been agreed and authorized by all relevant parties, e.g. customers, users, operations and support staff?*
- ✓ Do the plans include the release dates and deliverables and refer to related change requests, known errors and problems?
- ✓ *Have the impacts on costs, organizational, technical and commercial aspects been considered?*
- ✓ Have the risks to the overall services and operations capability been assessed?
- ✓ *Has there been a compatibility check to ensure that the configuration items that are to be released are compatible with each other and with configuration items in the target environments?*
- ✓ Have circumstances changed such that the approach needs amending?
- ✓ *Were the rules and guidance on how to apply it relevant for current service and release?*
- ✓ Do the people who need to use the plans understand and have the requisite skills to use them?
- ✓ *Is the service release within the SDP and the scope of the issues addressed by the transition model?*
- ✓ Has the service design altered significantly such that it is no longer appropriate?
- ✓ *Have potential changes in business circumstances been identified?*

Transition Planning and Support

Support

Support – work closely with Project support

Includes:

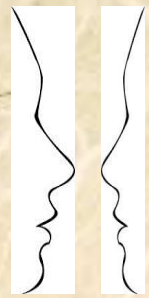
Administration
issues, risks, tools support

Communication
Communication plan, including target groups, differentiated content, frequency, channels, etc

Monitoring and reporting
Measuring and monitoring the release and deployment will establish whether the transition is proceeding according to plan

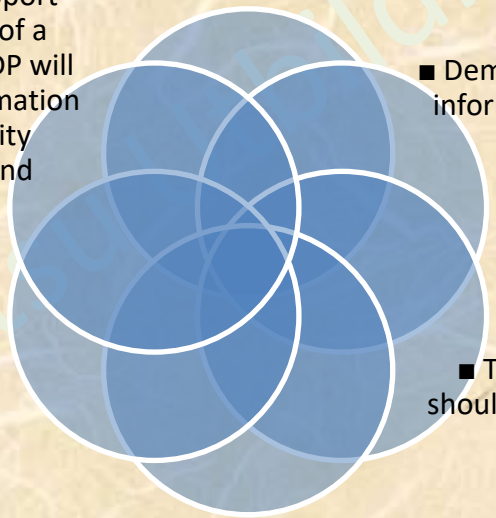
Transition Planning and Support

Interfaces



Transition planning and support has interfaces to almost every other area of service management:

■ Key inputs to transition planning and support come from the service design in the form of a service design package. Key inputs to this SDP will come from service level management, information security management, IT service continuity management, availability management and capacity management.



■ Demand management should provide long-term information about likely resource requirements.

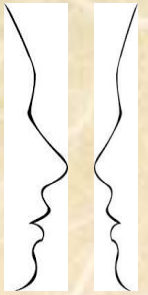
■ The service portfolio management process should engage transition planning and support to provide input to their planning and decisionmaking.

■ Business relationship management will help to manage appropriate two-way communication with customers.

■ Service portfolio management will submit a change proposal to trigger longer-term planning within transition planning and support.

Transition Planning and Support

Interfaces, cont



■ Supplier management will work during the service transition to ensure that appropriate contracts are in place.

■ All service transition processes are coordinated by transition planning and support, so service transition planning and support must have interfaces to change management, SACM, release and deployment management, service validation and testing, change evaluation and knowledge management.

■ Pilots, handover and early life support must be coordinated with the service operation functions.

■ Technical management and application management will provide the personnel needed to carry out many aspects of service transition, for example to review changes or plan deployments.

Transition Planning and Support

Information Management

Transition planning and support needs access to information about new or changed services to create and manage plans….

… such as guidelines, standards, models and plans, as well as documents created and maintained by other processes such as service design packages, contracts and operational level agreements (OLAs) and process documentation.

Transition Planning and Support

Critical Success Factors and KPIs

Critical Success Factor	KPI
Understanding and managing the tradeoffs between cost, quality and time	-Increase in the number of releases implemented that meet the customer's agreed requirements in terms of cost, quality, scope and release schedule (expressed as a percentage of all releases) -Reduced variation of actual versus predicted scope, quality, cost and time
Effective communication with stakeholders	-Increased customer and user satisfaction with plans and communications -Reduced business disruption due to better alignment between service transition plans and business activities
Identifying and managing risks of failure and disruption	-Reduction in number of issues, risks and delays -Improved service transition success rates
Coordinating activities of multiple processes involved in each transition	-Improved efficiency and effectiveness of the processes and supporting systems, tools, knowledge, information and data to enable the transition of new and changed services, e.g. sharing tool licences -Reduction in time and resource to develop and maintain integrated plans and coordination activities
Managing conflicting demands for shared resources	-Increased project and service team satisfaction with the service transition practices -Reduced number of issues caused by conflicting demands for shared resources.

Transition Planning and Support

Challenges

Coordinating and prioritizing many new or changed services can be a big challenge, especially if there are delays or test failures that cause projects to slip. Transition planning and support needs to understand the risks and issues for each project in order to proactively manage resource planning.

Transition Planning and Support

Risks

Risks to transition planning and support include:

- Lack of information from demand management and service portfolio management resulting in a reactive transition planning and support process with insufficient long-term planning
- Poor relationships with project and programme teams resulting in sudden and unexpected service transition requirements
- Delays to one transition having a subsequent effect on future transitions, due to resource constraints
- Insufficient information to prioritize conflicting requirements.

Change Management

Changes are made for a variety of reasons:

- Proactively, e.g. when organizations are seeking business benefits such as reduction in costs, improved services or increased ease and effectiveness of support
- Reactively as a means of resolving errors and adapting to changing circumstances.

Changes should be managed in order to:

- Optimize risk exposure (supporting the risk profile required by the business)
- Minimize the severity of any impact and disruption
- Achieve success at the first attempt
- Ensure that all stakeholders receive appropriate and timely communication about the change so that they are aware and ready to adopt and support the change

Change Management

Purpose

The purpose of the change management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

Change Management

Objectives

■ Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work.

■ Respond to the business and IT requests for change that will align the services with the business needs.

■ Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

■ Ensure that all changes to configuration items are recorded in the configuration management system.

■ Optimize overall business risk – it is often correct to minimize business risk, but sometimes it is appropriate to knowingly accept a risk because of the potential benefit.

Change Management

Scope

The scope of change management covers changes to all configuration items across the whole service lifecycle:

- Service solutions for new or changed services, including all of the functional requirements, resources and capabilities needed and agreed
- Management information systems and tools, especially the service portfolio, for the management and control of services through their lifecycle
- Technology architectures and management architectures required to provide the services
- Processes needed to design, transition, operate and improve the services
- Measurement systems, methods and metrics for the services, the architectures, their constituent components and the processes.

Excluded:

- Changes with significantly wider impacts than service changes, e.g. departmental organization, policies and business operations – these changes would produce RFCs to generate consequential service changes.
- Changes at an operational level such as repair to printers or other routine service components.

Change Management

Value to the business

$ Protecting the business, and other services, while making required changes

$ Implementing changes that meet the customers' agreed service requirements while optimizing costs

$ Contributing to meet governance, legal, contractual and regulatory requirements by providing auditable evidence of change management activity.

$ Reducing failed changes and therefore service disruption, defects and re-work

$ Reducing the number of unauthorized changes, leading to reduced service disruption and reduced time to resolve change-related incidents

$ Delivering change promptly to meet business timescales

Change Management

Value to the business, cont

$ Tracking changes through the service lifecycle and to the assets of its customers Contributing to better estimates of the quality, time and cost of change

$ Assessing the risks associated with the transition of services (introduction or disposal)

$ Improving productivity of staff by minimizing disruptions caused by high levels of unplanned or 'emergency' change and hence maximizing service availability

$ Reducing the mean time to restore service (MTRS), via quicker and more successful implementations of corrective changes

$ Liaising with the business change process to identify opportunities for business improvement.

Change Management

Policies

- Zero tolerance for unauthorized change
- Align with business, project and stakeholder change management processes
- Ensure that changes create business value and that the benefits for the business created by each change are measured and reported
- Prioritization (innovation, prevention, correction)
- Single focal point for changes
- Access authorization
- Integration with other SM processes
- Change windows usage
- Performance measures for the process

Change Management

Principles, basic concepts

Comply with relevant legislation, industry codes of practice, standards and organizational practices

Design identification and classification rules and methods

Include in the process accountabilities and responsibilities of all stakeholders

Include in the process independent testing and formal evaluation of change

Define escalation routes and methods, authorisation flows

Define the composition of advisory boards, (CAB) and the emergency CAB (ECAB)

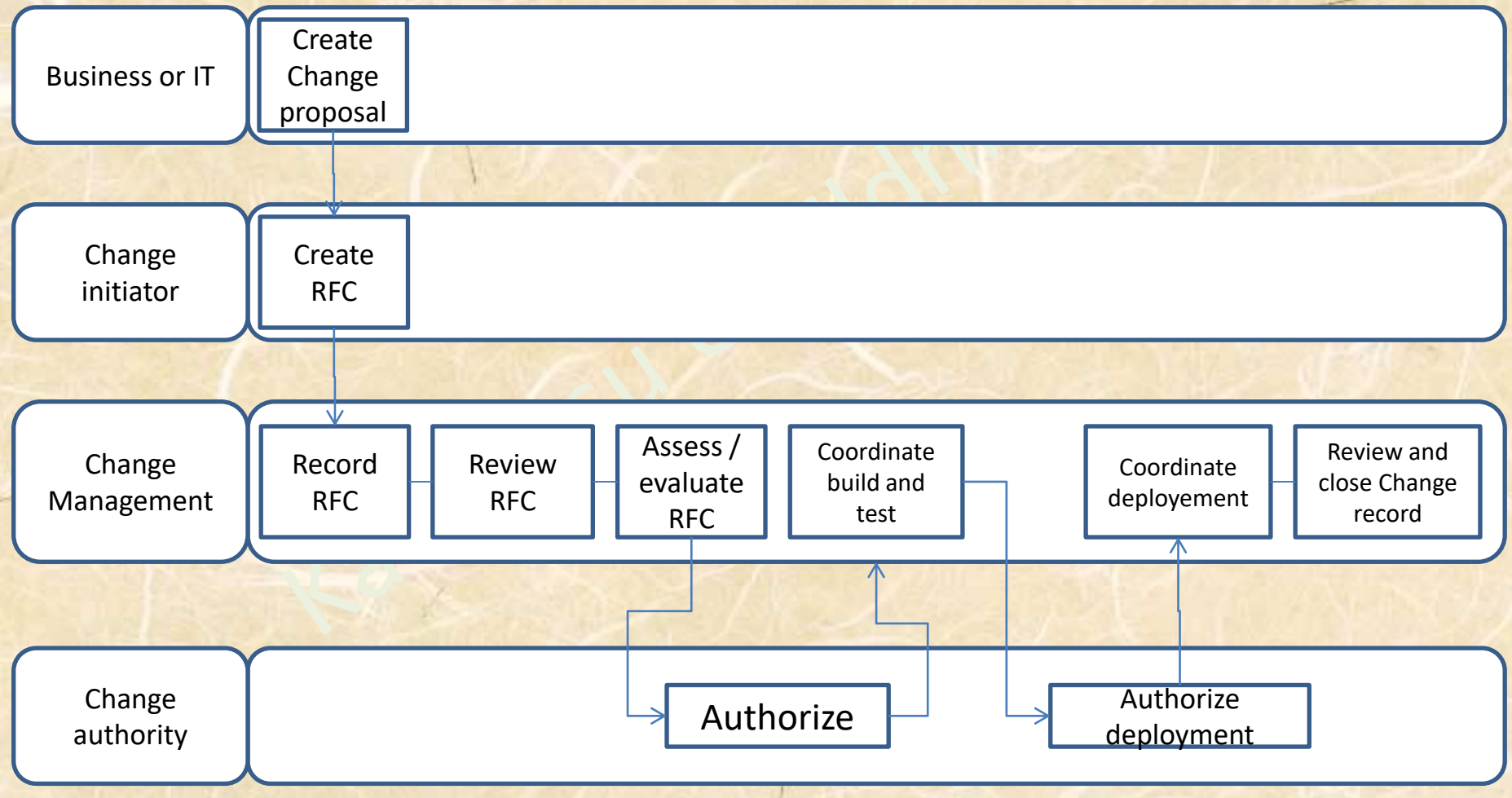
Design for communicating changes, change schedule and release plans

Design procedures for:

Methods of raising an RFC, tracking and management of change requests, identification of dependencies and incompatibilities between changes, verification of the implementation of a change, oversight and evaluation of deliverables from change and release implementation, measurement and reporting of change success and business value created, regular review of changes to identify trends and improvements, ….

Change Management

Flow, activities



Change Management

Activities

- Planning and controlling changes
- Change and release scheduling (working with release and deployment management)
- Communications
- Change decision-making and change authorization
- Ensuring that remediation plans are in place
- Measurement and control
- Management reporting
- Understanding the impact of change
- Continual improvement.

Change Management

Change types

Request	Trigger	Change type
Request for change to service portfolios	New / changed portfolio line	Normal change
Request for change to service or service definition	To existing or planned service Attributes, service improvement	
Project change proposal	Business change	Project Change Management
User access request, user service request	Request Fullfillment	Standard change
Operational activity	Maintenance	Standard change
Operational repair, Emergency change	Incident Management, Event Management	Standard change, Emergency change

Change Management

Change model

A change model is a way of predefining the steps that should be taken to handle a particular type of change in an agreed way. Support tools can then be used to manage the required process. This will ensure that such changes are handled in a predefined path and to predefined timescales.

Emergency changes	May have different authorization and may be documented retrospectively
Security patches	May require specific testing and guaranteed deployment to large numbers of targets, some of which may not be online
Service requests	May not require specific authorisation and may be automated

A change model will include procedures, timescales, escalation routes, roles, responsibilities and resource descriptions.

Change Management

Remediation

Oooooops!

A change might not be successfull. Ideally, a backout procedure can be applied , but not all changes are reversible.

When planning a change, the triggers or decision milestones for the need of remediation are included.

Change Management

Artifacts, outputs

Some examples of artifacts / outputs
Continually updated RFC and Change records
Change authority decisions, e.g. MoM
Work orders
Change evaluation reports
Change schedules
Updated configuration items
Predicted Service Outage
Financial considerations
Risk management plan

Change Management

Triggers

Trigger	
Strategic	Legal/regulatory change
	Organizational change
	Policy and standards change
	Change after analysing business, customer and user activity patterns
	Addition of new service to the market space
	Updates to the service portfolio
	Change of sourcing model
	Technology innovation

Change Management

Triggers

Trigger	
Service change	Service package
	Release package
	Changed Service Level Requirements
	Physical change in the environment
	Warranty and Utility triggers
	Decommission / retire services
	Process, procedure, documentation changes
	Measurement system / supporting tool changes
	Continual Service Improvement initiatives

Change Management

Triggers

Trigger	
Operational change	Maintenance
	Incident / problem resolution
	Proactivity (e.g. Security, proactive problem management)
	Standard changes (Request fulfillment)

Change Management

Inputs

Policy and strategy for change and release
Request for change
Change proposal
Plans – change, transition, release, test, evaluation and remediation
Current change schedule and PSO
Evaluation reports and interim evaluation reports
Current assets or configuration items
Test results, test report and evaluation report
Knowledge

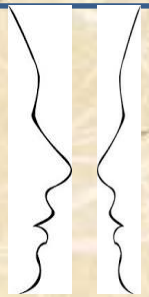
Change Management

Outputs

Authorized changes
Authorized change proposals
Change to the services, service or infrastructure resulting from authorized changes
New, changed or disposed configuration items, e.g. baseline, service package, release package
Revised change schedule
Revised PSO
Authorized change plans
Change decisions and actions
Change documents and records
Change management reports.
Rejected and cancelled RFCs

Change Management

Interfaces



Business change processes - The service portfolio management process will submit change proposals to change management before chartering new or changed services, in order to ensure that potential conflicts for resources or other issues are identified.

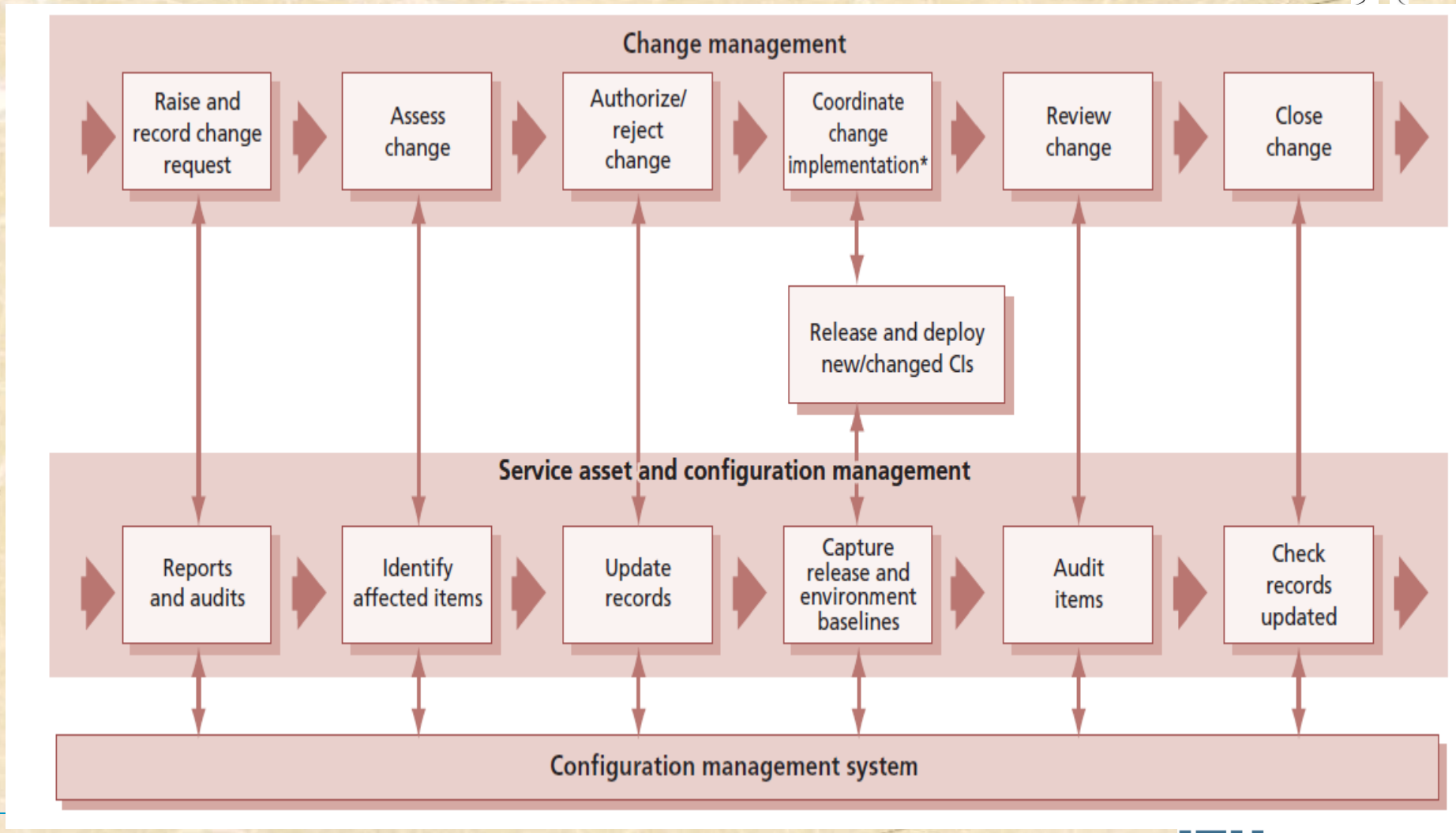
Sourcing and partnering - Sourcing and partnering arrangements should clearly define the level of autonomy a partner may have in effecting change within their service domain without reference to the overall service provider.

Programme and project management - ensure that the change schedule is effective and that all changes are well managed

Organizational and stakeholder change Management – chapter 5

Change Management

Interfaces, SACM



Change Management

Interfaces, cont

Interfacing ITSM process	What and How
Problem management	Problem management is one of the major sources of RFCs and is also often a major contributor to CAB discussion.
IT service continuity management	Procedures and plans, which should be updated via change management
Information security management	Security will be a key contributor to CAB discussion on many services. Every significant change will be assessed for its potential impact on information security management.
Capacity management and demand management	Changes arising from capacity management, including those set out in the capacity plan, will be initiated as RFCs through the change process.
Service portfolio management	Change proposals will be a significant input to long-term planning for the change schedule. Some change requests will require analysis by the service portfolio management process, potentialy adding to the service pipeline

Change Management

Information Management

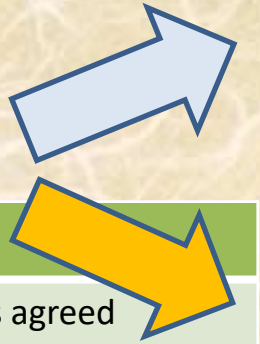
All change requests must be associated with services and other CIs.
This means that either

- they must be included within the CMS or
- a mechanism must be provided to enable cross referencing and searching changes related to CIs.

Correlate changes with incidents and review the history of changes to any CI as part of incident or problem management.

Change Management

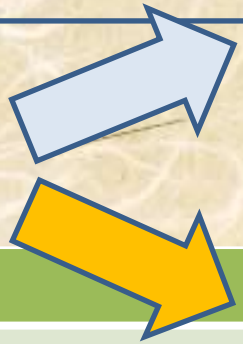
Critical success factors, KPIs



Critical Success Factor	KPI
Responding to business and IT requests for change that will align the services with the business needs while maximizing value	**Increase in the percentage of** changes that meet the customer's agreed requirements, e.g. quality/cost/time **The benefits of change (expressed as** 'value of improvements made' + 'negative impacts prevented or terminated') exceed the costs of change **Reduction in the backlog** of change requests **Average time to implement meets SLA** targets, based on urgency/priority/change type **Increase in accuracy of predictions** for time, quality, cost, risk, resource and commercial impact **Increase in scores in survey of** stakeholder satisfaction for the change management process

Change Management

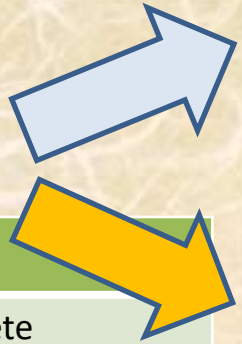
Critical success factors, KPIs



Critical Success Factor	KPI
Optimizing overall business risk	**Reduction in the number of disruptions** to services, defects and re-work caused by inaccurate specification, poor or incomplete impact assessment **Reduction in the percentage of changes** that are categorized as emergency changes **Increase in change success rate** (percentage of changes deemed successful at review/number of changes authorized) **Reduction in the number of changes** where remediation is invoked **Reduction in the number of failed** Changes **Reduction in the number of** unauthorized changes identified **Reduction in the number of incidents** attributed to changes

Change Management

Critical success factors, KPIs



Critical Success Factor	
Ensuring that all changes to configuration items are well managed and recorded in the configuration management system	**Reduction in the number and** percentage of changes with incomplete change specifications **Reduction in the number and** percentage of changes with incomplete impact assessments **Reduction in number of audit** compliance issues for the change management process **KPI Reduction in number and percentage** of discrepancies found by service asset and configuration management verification and audit.

Change Management

Challenges

Ensuring that every change is recorded and Managed

Change management process must be seen to facilitate change, rather than to introduce delays. A change management process that is regarded as bureaucratic and time-wasting will not be valued.

There can be a significant challenge to agree and document the many levels of change authority that are needed to manage change effectively and to communicate effectively between these change authorities.

Change Management

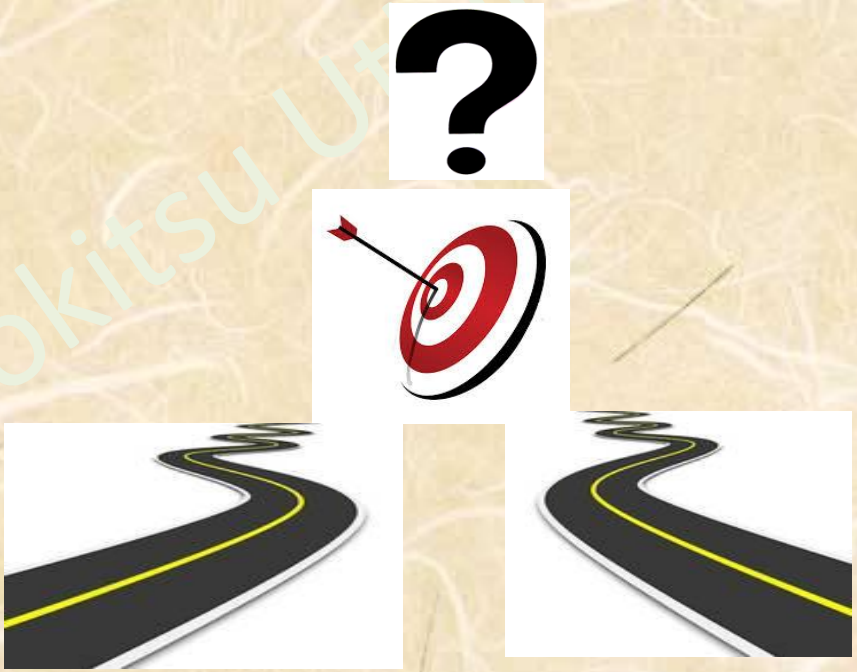
Risks

- Lack of commitment to the change management process
  - by the business, and lack of business sponsorship
  - by IT management, and lack of IT management sponsorship
  - by IT staff
- Implementation of changes without the use of change management
- Change assessment being reduced to box ticking, without real consideration of the risks, costs and benefits
- Introduction of delays to change implementation without adding sufficient value
- Insufficient time being allowed for proper assessment of changes, and pressure from projects or the business to expedite decisions
- Insufficient time allowed for implementation of changes, and attempts to fit too many changes into a change window
- Insufficient resources for assessment, planning and implementation of the number of changes required by the business
- Lack of clarity on how change management should interact with other service management processes, such as release and deployment management or service asset and configuration management
- Lack of clarity on how change management should interact with project management or service design activities
- Excessively bureaucratic change management processes that introduce excessive delay to required changes.

Service Asset and Configuration Management

Purpose

The purpose of the SACM process is to ensure that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed.



Service Asset and Configuration Management

Objectives

■ Ensure that assets under the control of the IT organization are identified, controlled and properly cared for throughout their lifecycle.

■ Identify, control, record, report, audit and verify services and other configuration items (CIs).

■ Account for, manage and protect the integrity of Cis

■ Ensure the integrity of CIs by establishing and maintaining an accurate and complete configuration management system (CMS).

■ Maintain accurate configuration information on the historical, planned and current state of services and other CIs.

■ Support efficient and effective service management processes

Service Asset and Configuration Management

Value to business

SACM provides visibility of accurate representations of a service. This enables:

$ Better forecasting and planning of changes

$ Resolution of incidents and problems within the service level targets

$ More business opportunities as the service provider is able to demonstrate control of assets and services

$ Traceability of changes from requirements

$ The ability to identify the costs of a service

$ Reduced cost and time to discover configuration information when it is needed

$ Proper stewardship of fixed assets that are under the control of the service provider.

Service Asset and Configuration Management

Scope

The scope of SACM includes management of the complete lifecycle of every CI.
Every CI is a service asset, but many service assets are not CIs.
Also, information that is stored on the server but is not under the control of change management may be a very valuable asset, but it is not a configuration item.

The scope includes interfaces to internal and external service providers where there are assets and configuration items that need to be controlled, e.g. shared assets.

Service Asset and Configuration Management

Policies

Policies set the objectives, scope, principles and critical success factors

SACM policies are related to the Change Management and Release and Deployment Management policies

Specific Asset Management policies may apply.

Service Asset and Configuration Management

Principles

Find a balance between costs and resources and the risks with maintaining a accurate Configuration Management System.

A general rule for the level of detail required is that you should not include attributes or relationships unless these create more value than it costs to maintain them.

Service Asset and Configuration Management

Basic concepts

Distinguish between service assets, configuration items and configuration records

A service asset ….	…is any resource or capability that could contribute to the delivery of a service
A **configuration item (CI) …**	…is a service asset that needs to be managed in order to deliver an IT service
A **configuration record …**	…is a set of attributes and relationships about a CI
The **service knowledge management system** (SKMS) …	…is a set of tools and databases that are used to manage knowledge, information and data. The SACM process is not responsible for managing the SKMS.

Service asset and configuration management delivers a model of the services, assets and the infrastructure by recording the relationships between configuration items

Service Asset and Configuration Management

Configuration model

A well balanced configuration model enables

To assess:

- the impact and cause of incidents and problems
- the impact of proposed changes

To plan:

- and design new or changed services
- technology refresh and software upgrades
- releases and migrate service assets to different locations and service centres

To optimize:

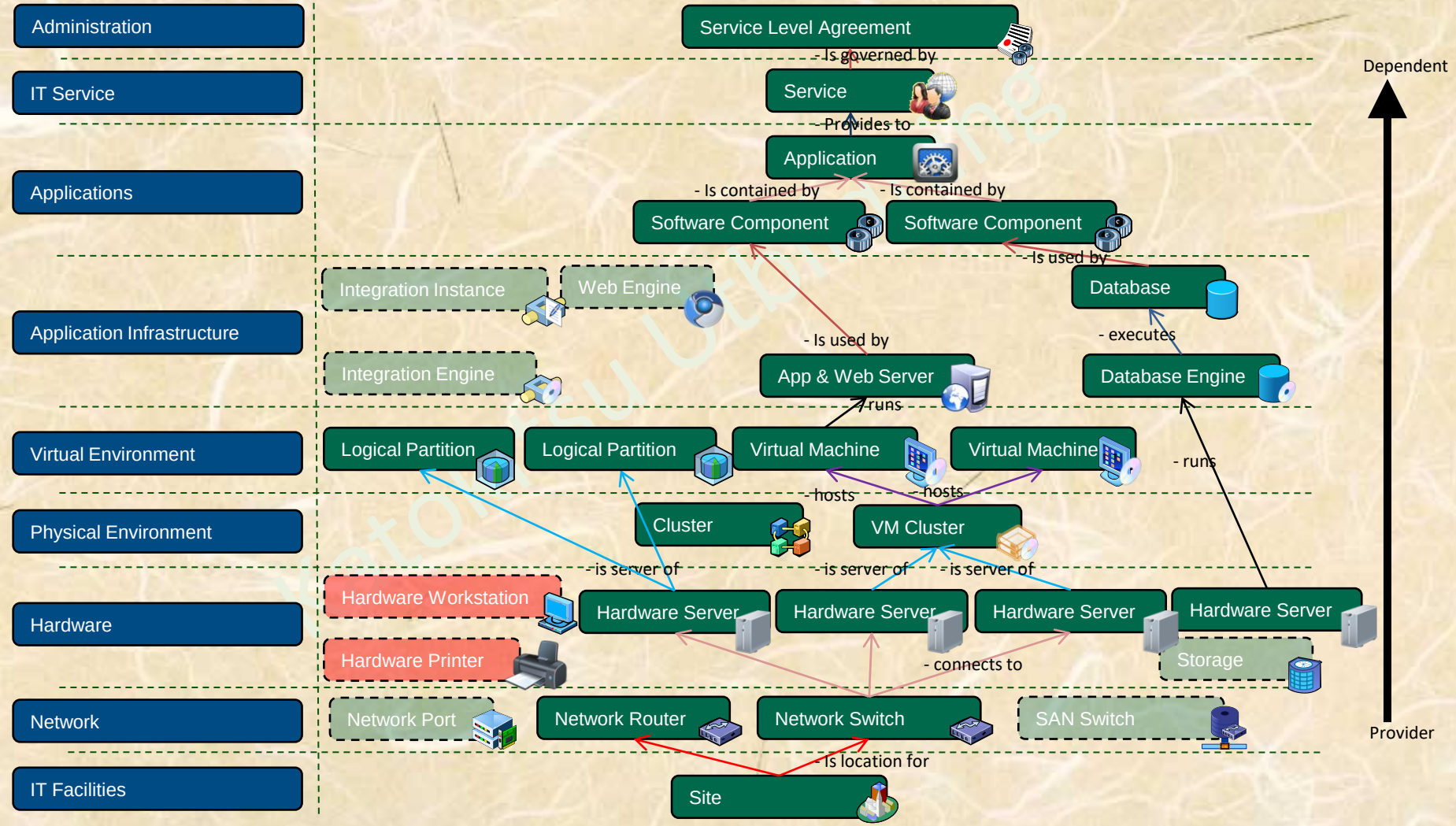
- asset utilization and costs, e.g. consolidate data centres, reduce variations and re-use assets.

Service Asset and Configuration Management

CI types

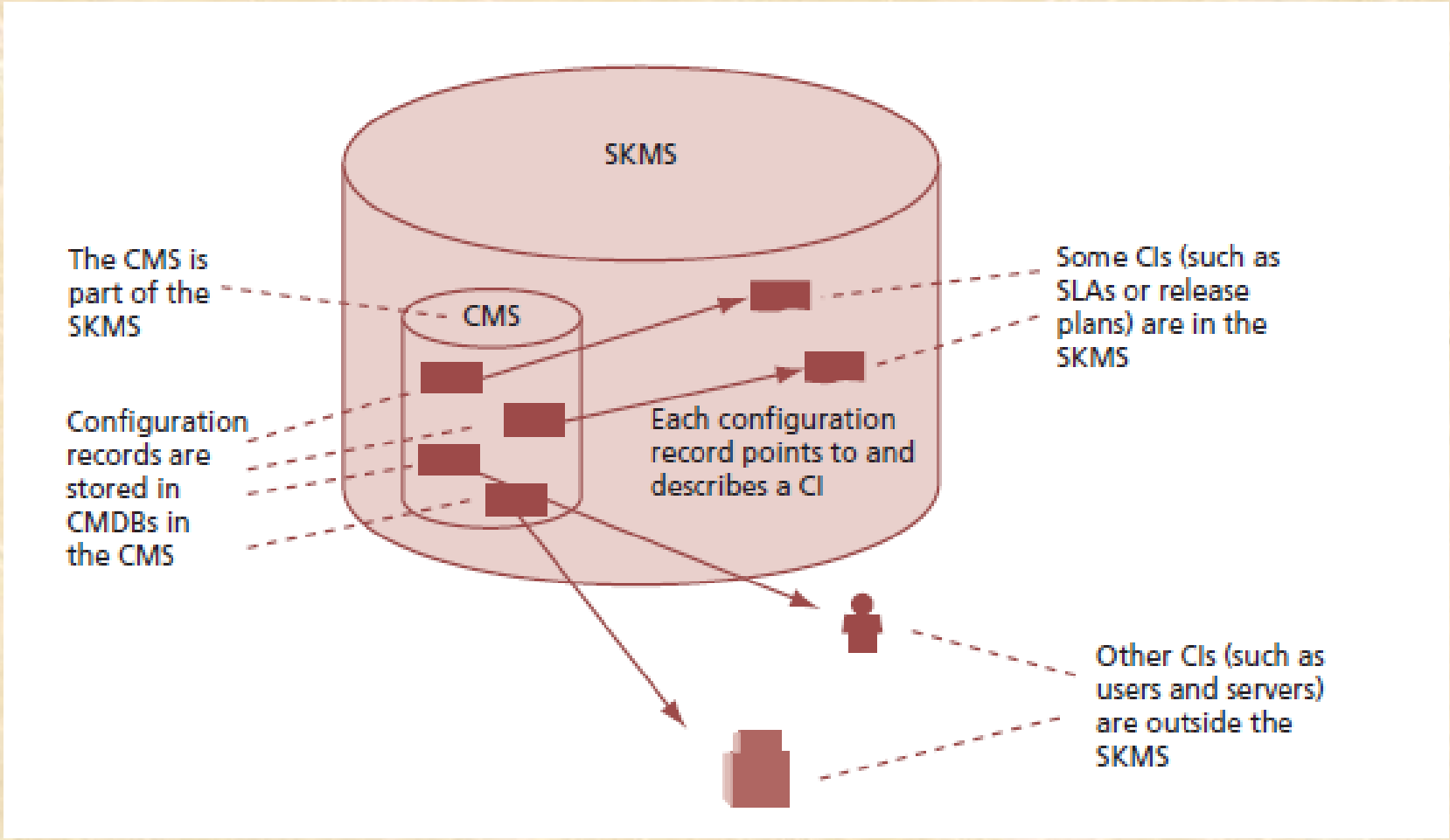
Service Lifecycle CI	business case, service management plans, service lifecycle plans, service design package, release and change plans and test plans.
Service CI	Service capability assets: management, organization, processes, knowledge, people ● Service resource assets: financial capital, systems, applications, information, data, infrastructure and facilities, financial capital, people ● Service model ● Service package ● Release package ● Service acceptance criteria.
Organisation CI	●The organization's business strategy or other policies that are internal to the organization but independent of the service provider ●Regulatory or statutory requirements ●Products shared among more than one group
Internal CI	Delivered by individual projects, including tangible (data centre) and intangible assets such as software that are required to deliver and maintain the service and infrastructure.
External CI	External customer requirements and agreements, releases from suppliers or sub-contractors and external services
Interface CI	Required to deliver the end-to-end service across a service provider interface (SPI), for example an escalation procedures / rules document

Service Asset and Configuration Management



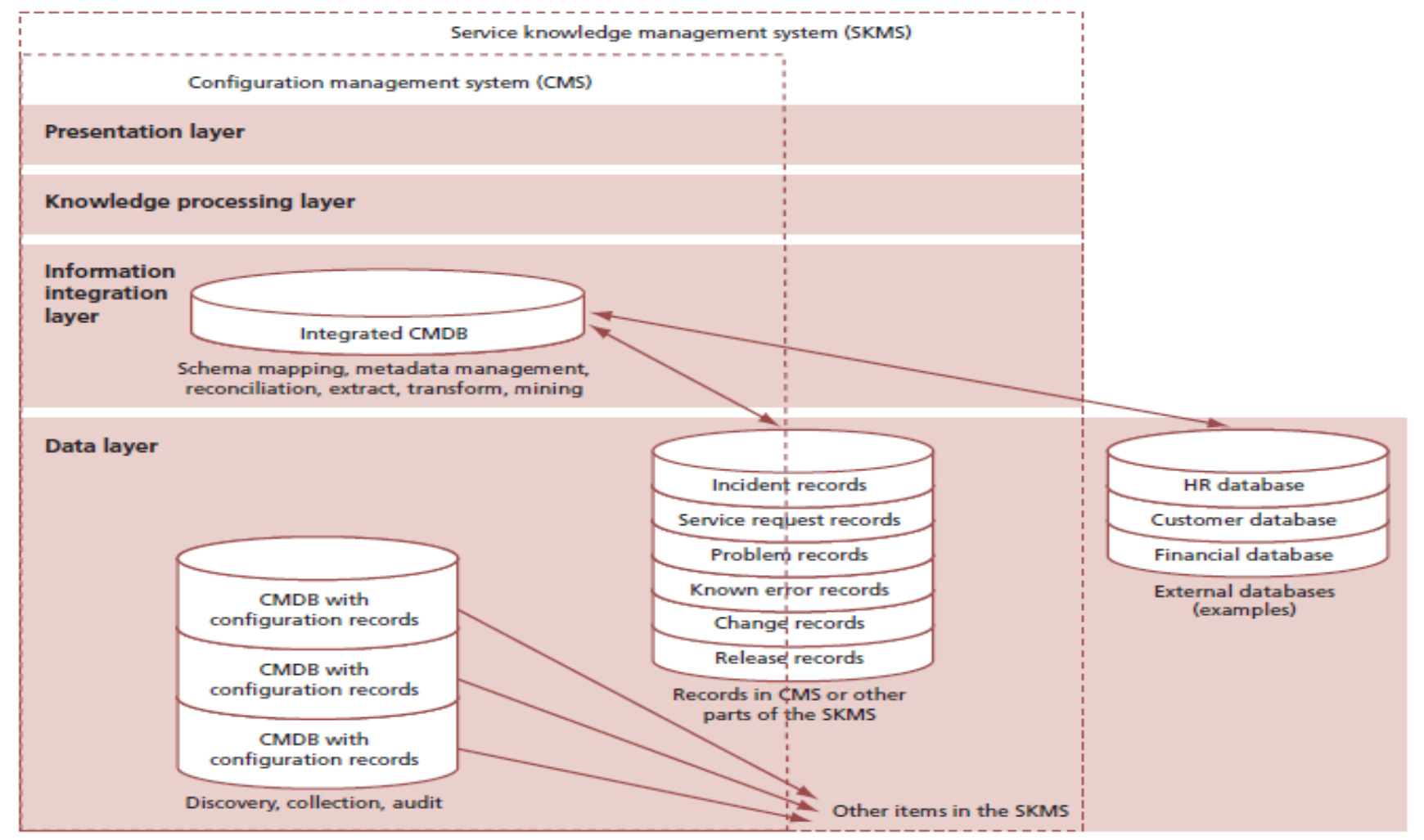
Service Asset and Configuration Management

CMS



Service Asset and Configuration Management

CMS



Service Asset and Configuration Management

CMS presentation layers

Change and release view	Used by personnel responsible for change management and release and deployment management
Technical configuration view	Used to support the needs of personnel in technical and application management functions
Service desk view	For use by the service desk, for example when logging and managing incidents and service requests
Configuration lifecycle view	Used by service asset and configuration management personnel who are responsible for managing the lifecycle of configuration items.

Service Asset and Configuration Management

Configuration baseline

A 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.

Service Asset and Configuration Management

Snapshot

A 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. Sometimes this is referred to as a *footprint.*

Service Asset and Configuration Management

Asset management

Fixed assets of an organization are assets which have a financial value, can be used by the organization to help create products or services and have a long-term useful life.

Some activities:

- Identifying each asset, including unique naming and labels
- Identifying and recording asset owners
- Maintaining an asset register that includes details of all fixed assets
- Understanding the purchase cost, depreciation and net book value of each asset
- Helping to protect the assets from damage, theft etc. (physical and logical security controls)
- Carrying out regular audits to ensure the integrity of fixed assets.

Service Asset and Configuration Management

Software asset management, SAM

Software asset management (SAM) is responsible for the management of software, software licences and codes for activating software.

Risks:

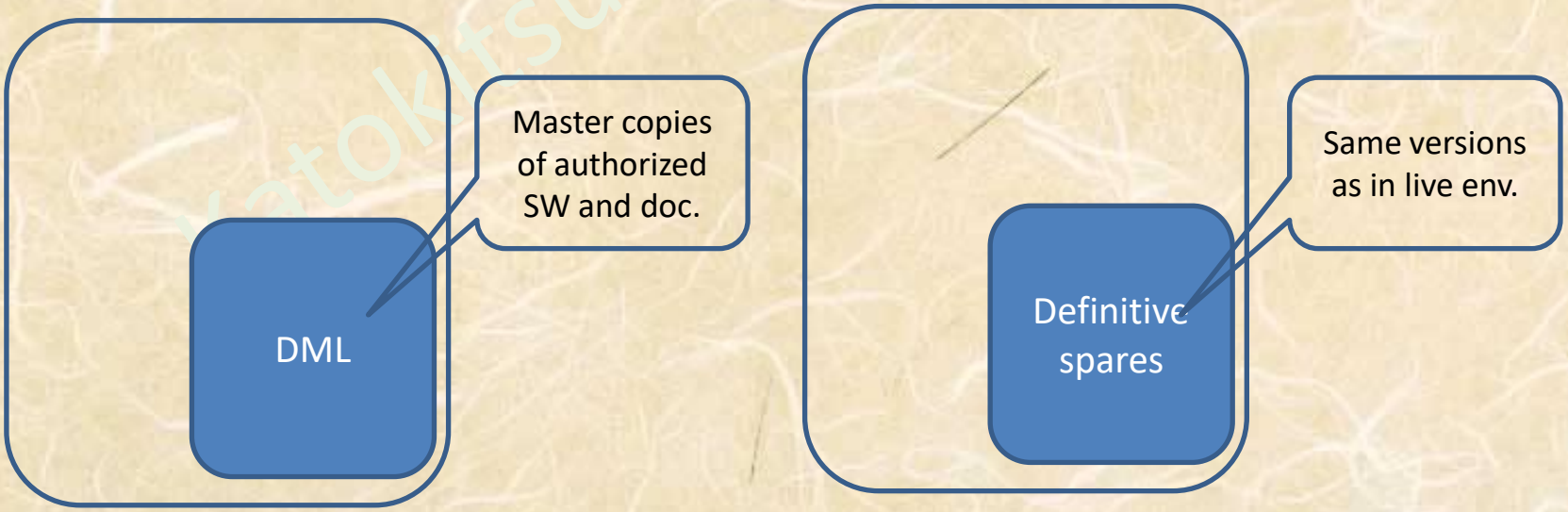
- Software being used without licences being purchased
- Loss of proof of licences which have been purchased
- Terms and conditions being breached unknowingly
- Purchasing more licences than are needed and not being aware that these are under-utilized.

Service Asset and Configuration Management

Secure libraries and secure stores

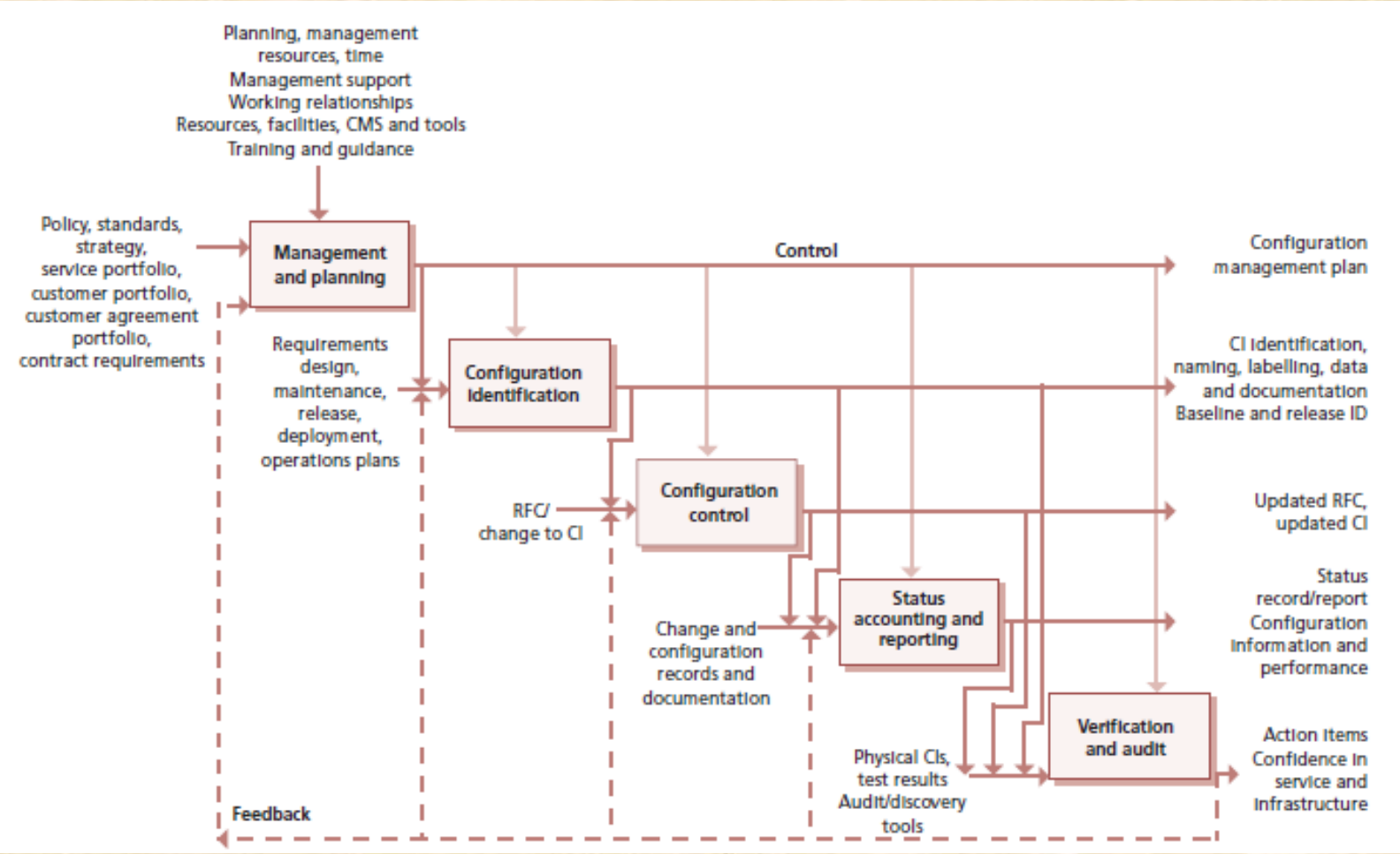
A **secure library** is a collection of software, electronic or document CIs of known type and status. Access to items in a secure library is restricted. Libraries are used for controlling and releasing components throughout the service lifecycle, e.g. in design, building, testing, deployment and operation.

A **secure store** is a location that warehouses IT assets.



Service Asset and Configuration Management

Activities, methods, techniques



Service Asset and Configuration Management

Management and Planning

Compile a Configuration Management Plan, including

- Scope
  - Applicable services, locations, environment
- Requirements
  - Policies, business, Service Management, contractual requirements, accountability, traceability, auditability
- Applicable standards
  - E.g. ISO20000
- Organisation for SACM
  - Roles, responsibilities, CAB, authorisation
- SACM system and tools
  - Processes, procedures, tools, implementation, identification, baselines
- Interfaces to other processes, functions
  - Asset management, development, service providers, service desk

Service Asset and Configuration Management

Identification

- Define criteria for selection
  - Include also services, service components, release packages, tools, etc
- Discover / select items
  - Define structure, model, level – top-down method
- Assign / Name / label Cis
  - Unique, aligned with existing conventions, versions, future growth
- Specify attributes
  - CI type, name, version, date, license details, status, audit data, baseline
- Identify owner
  - Owner, relations, supplier, SLA referens

Service Asset and Configuration Management

Control

No CI should be added, modified, replaced or removed without an appropriate controlling documentation or procedure being followed.

Policies and procedures for:

- License control
- Version control
- Change Management
- Access control
- Integrity control and protection

Service Asset and Configuration Management

Status accounting and reporting

The method by which CIs move from one state to another should be defined: e.g. an application release may be registered, accepted, installed or withdrawn.

E.g., the status change from Accepted to Installed could be governed by the Release and Deployment process.

The CMS should be updated with the reason, date-time stamp and person or automatism that made the status change.

Service Asset and Configuration Management

Status accounting and reporting

Typical reports include:

- A list of product configuration information included in a specific configuration baseline
- A list of configuration items and their configuration baselines
- Details of the current revision status and change history
- Status reports on changes, waivers and deviations, including unauthorized changes
- Details of the status of delivered and maintained products concerning part and traceability numbers
- Report on unauthorized usage of hardware, software or other CIs

Service Asset and Configuration Management

Verification and auditing

Conduct audits to check that the CMDB and related configuration information is consistent with the physical state of all Cis.

These audits should verify that correct and authorized versions of CIs exist (and that only such CIs exist) and are in use.

Unregistered and unauthorized items that are discovered during configuration audits should be investigated and corrective action taken to address possible issues with procedures and the behaviour of personnel.

Service Asset and Configuration Management

Triggers

- Updates from change management
- Updates from release and deployment management
- Purchase orders
- Acquisitions
- Service requests.

Service Asset and Configuration Management

Inputs

- Designs, plans and configurations from service design packages
- Requests for change and work orders from change management
- Actual configuration information collected by tools and audits
- Information in the organization's fixed asset register.

Service Asset and Configuration Management

Outputs

- New and updated configuration records
- Updated asset information for use in updating the fixed asset register
- Information about attributes and relationships of configuration items, for use by all other service management processes. This information should be presented in appropriate views for each audience.
- Configuration snapshots and baselines
- Status reports and other consolidated configuration information
- Audit reports.

Service Asset and Configuration Management

Interfaces

■ Change management – identifying the impact of proposed changes

■ Financial management for IT services – capturing key financial information such as cost, depreciation methods, owner and user (for budgeting and cost allocation), maintenance and repair costs

■ ITSCM – awareness of the assets on which the business services depend, control of key spares and software

■ Incident/problem/error – providing and maintaining key diagnostic information; maintenance and provision of data to the service desk

■ Availability management

Service Asset and Configuration Management

Information management

- Backup – frequency, location
- Retention – how long, how much
- Housekeeping – reduntant information
- Pointers to SKMS – verify.
- SKMS – same accuracy as CMS

Service Asset and Configuration Management

Critical success factors, KPIs

Critical Success Factor	KPI
Accounting for, managing and protecting the integrity of CIs	Improved accuracy in budgets and charges for the assets utilized by each customer or business unit Increase in re-use and redistribution of under-utilized resources and assets Reduction in the use of unauthorized hardware and software, non-standard and variant builds that increase complexity, support costs and risk to the business services Reduced number of exceptions reported during configuration audits
Supporting service management processes by providing accurate configuration information at the right time	Percentage improvement in maintenance scheduling over the life of an asset (not too much, not too late) Reduction in the average time and cost of diagnosing and resolving incidents and problems Improvement in time to identify poorperforming and poor-quality assets Reduction in risks due to early identification of unauthorized change Reduced percentage of changes not completed successfully or causing errors because of poor impact assessment, incorrect data in the CMS, or poor version controled licences against paid-for licences
CSF Establishing and maintaining an accurate and complete configuration management system (CMS)	Reduction in business impact of outages and incidents caused by poor service asset and configuration management Increased quality and accuracy of configuration information Improved audit compliance Shorter audits as quality configuration information is easily accessible Fewer errors caused by people working with out-of-date information.

Service Asset and Configuration Management

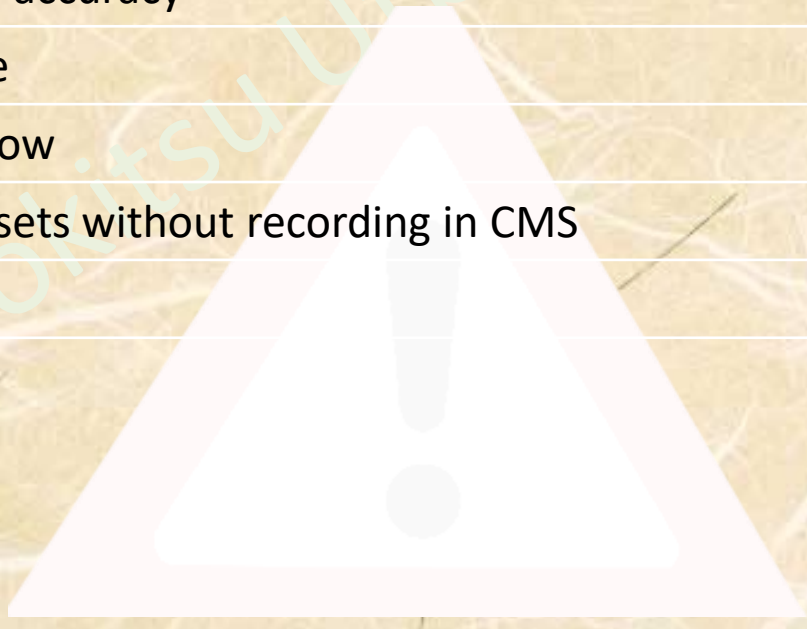
Challenges

- Persuading technical support staff to adopt a checking in/out policy
- Attracting and justifying funding for SACM
- 'just collecting data because it is possible to do'
- Lack of commitment and support from management

Service Asset and Configuration Management

Risks

Technical focus
Degradation of accuracy
Scope too wide
Scope too narrow
Moving HW assets without recording in CMS



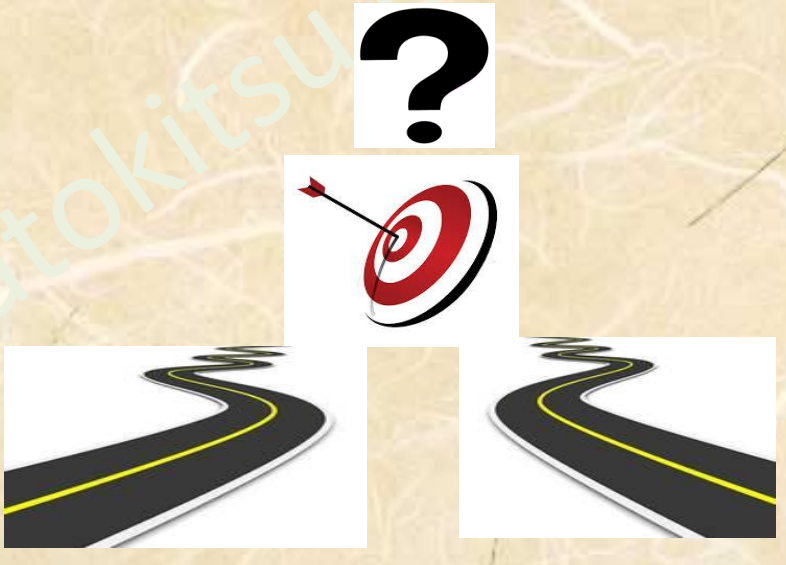
Release and Deployment Management

Purpose

The purpose of the release and deployment management process is

- to plan, schedule and control the build
- test and deployment of releases
- to deliver new functionality required by the business

while protecting the integrity of existing services.



Release and Deployment Management

Objectives

■ Define and agree release and deployment management plans with customers and stakeholders

■ Create and test release packages that consist of related configuration items that are compatible with each other

■ Ensure that the integrity of a release package and its constituent components is maintained throughout the transition activities, and that all release packages are stored in a DML and recorded accurately in the CMS

■ Deploy release packages from the DML to the live environment following an agreed plan and schedule

■ Ensure that all release packages can be tracked, installed, tested, verified and/or uninstalled or backed out if appropriate

■ Ensure that organization and stakeholder change is managed during release and deployment activities

Release and Deployment Management

Objectives, cont

■ Ensure that a new or changed service and its enabling systems, technology and organization are capable of delivering the agreed utility and warranty

■ Record and manage deviations, risks and issues related to the new or changed service and take necessary corrective action

■ Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities

■ Ensure that skills and knowledge are transferred to service operation functions to enable them to effectively and efficiently deliver, support and maintain the service according to required warranties and service levels.

Release and Deployment Management

Value to business

Adds value to the business by:

- Delivering change, faster and at optimum cost and minimized risk
- Assuring that customers and users can use the new or changed service in a way that supports the business goals
- Improving consistency in implementation approach across the business change, service teams, suppliers and customers
- Contributing to meeting auditable requirements for traceability through service transition.

Release and Deployment Management

Scope

The scope of release and deployment management includes:

- the processes, systems and functions to package, build, test and deploy a release
- establish the service specified in the service design package
- formally hand the service over to the service operation functions

The scope includes all configuration items required to implement a release

Release and Deployment Management

Policies, principles and basic concepts

- Focus on stability or speed
- Testing requirements
- Release frequency, agility
- Release units size and content
- Naming conventions
- Costs (automation, geography, resources)
- Criticality

Release and Deployment Management

Release unit and release package

A release unit describes the portion of a service or IT infrastructure that is normally released as a single entity.

A release package is a set of configuration items that will be built, tested and deployed together as a single release.

Where possible, release packages should be designed so that some release units can be removed if they cause issues in testing.

Release and Deployment Management

Deployment options

Big Bang - The new or changed service is deployed to all user areas in one operation

Phased - The service is deployed to a part of the user base initially, and then this operation is repeated to the entire user base.

Push method - A push approach is used where the service component is deployed from the centre and pushed out to the target locations

Pull method - A pull approach is 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 user workstation restarts.

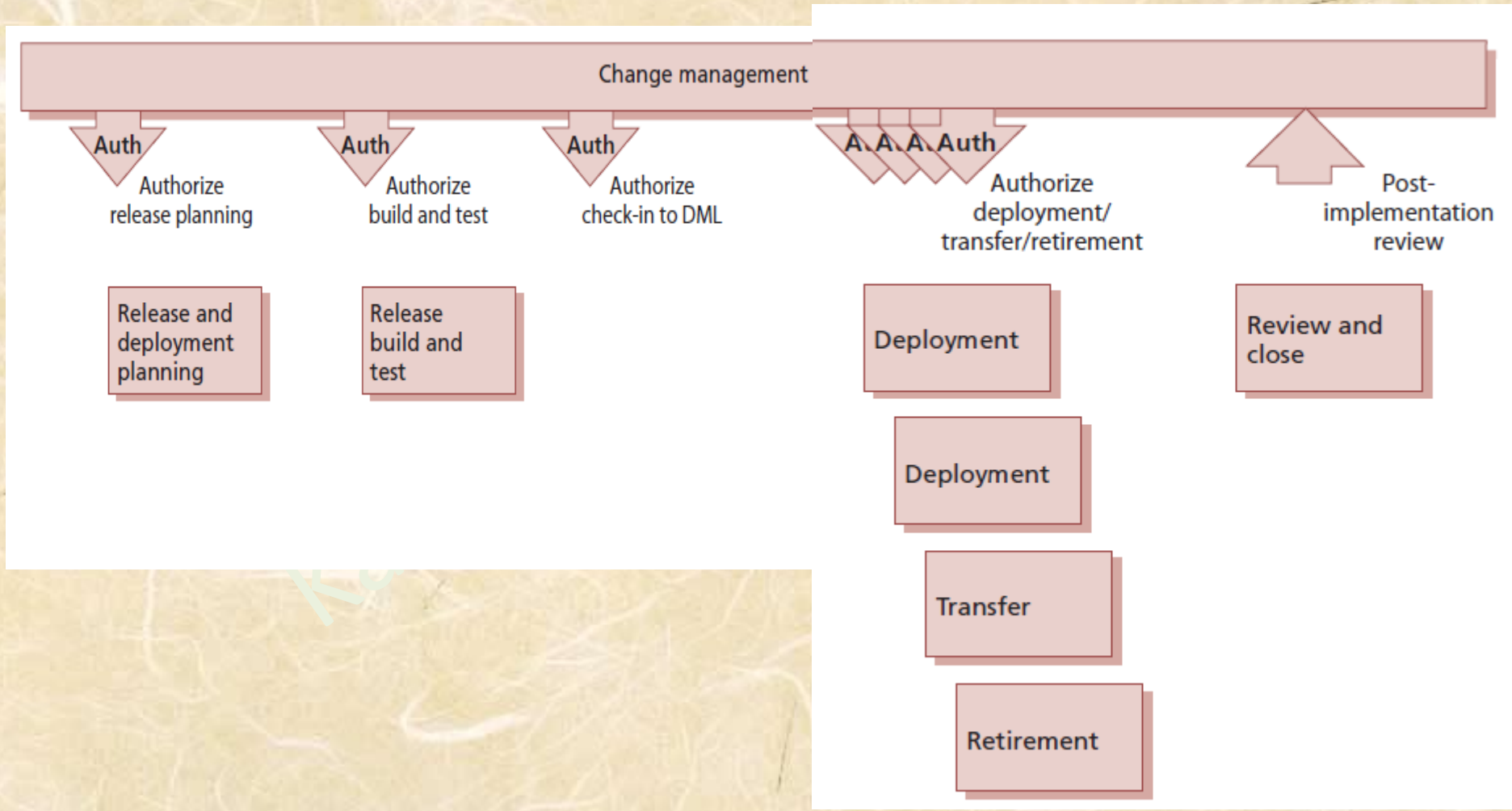
Release and Deployment Management

Considerations

■ Verify that a release complies with the SDP
■ Ensure the integrity of hardware and software is protected during installation, handling, packaging and delivery
■ Use standard release and deployment procedures and tools
■ Automate the delivery, distribution, installation, build and configuration audit procedures where appropriate to reduce costly manual steps
■ Manage and deploy/re-deploy/remove/retire software licences
■ Package and build the release package so that it can be backed out or remediated if required
■ Use SACM procedures, the CMS and DML to manage and control components during release and deployment management activities
■ Document the release and deployment management steps
■ Document the deployment group or target environment that will receive the release
■ Issue service notifications
■ Implement controls and checklists to ensure that all required activities take place and that records are maintained to support future audits of the process.

Release and Deployment Management

Process activities, methods



Release and Deployment Management

Process activities, methods

■ **Release and deployment planning**
Plans for creating and deploying the release are created.
This phase starts with change management authorization to plan a release and ends with change management authorization to create the release.

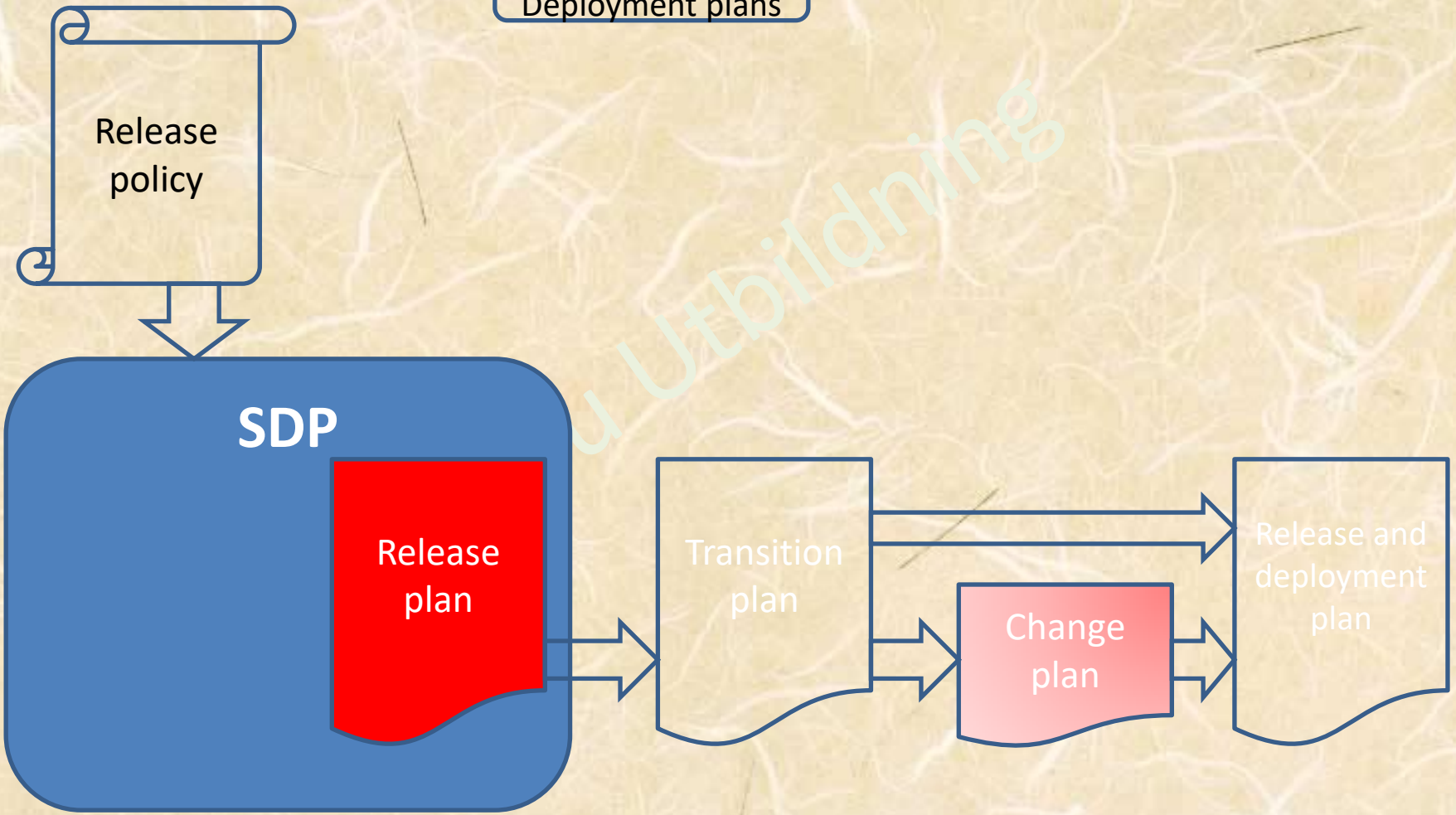
■ **Release build and test**
The release package is built, tested and checked into the DML. This phase starts with change management authorization to build the release and ends with change management authorization for the baselined release package to be checked into the DML by service asset and configuration management. This phase only happens once for each release.

■ **Deployment**
The release package in the DML is deployed to the live environment. This phase starts with change management authorization to deploy the release package to one or more target environments and ends with handover to the service operation functions and early life support. There may be many separate deployment phases for each release, depending on the planned deployment options.

■ **Review and close**
Experience and feedback are captured, performance targets and achievements are reviewed and lessons are learned.

Release and Deployment Management

Release and Deployment plans



Release and Deployment Management

Plan content

Scope and content of the release
Risk assessment and risk profile for the release
Organizations and stakeholders affected by the release
Stakeholders that may authorize the change request for each stage of the release
Team responsible for the release
Deployment schedule for the release
Approach to working with stakeholders and deployment groups to determine: ● Delivery and deployment strategy ● Resources for the release build, test and deployment, and for early life support ● Amount of change that can be absorbed.

Release and Deployment Management

Pass / Fail criteria

Defined for each authorization point through release and deployment management.

e.g.

Pass: All tests are completed successfully

Fail:

- Insufficient resources to pass to the next stage.
- Service operation does not have capabilities.
- Service design does not conform to the service operation standards.
- Service acceptance criteria are not met.
- Mandatory documents are not signed off.
- SKMS and CMS are not updated.
- The incidents, problems and risks are higher than predicted.

Release and Deployment Management

Build and test planning

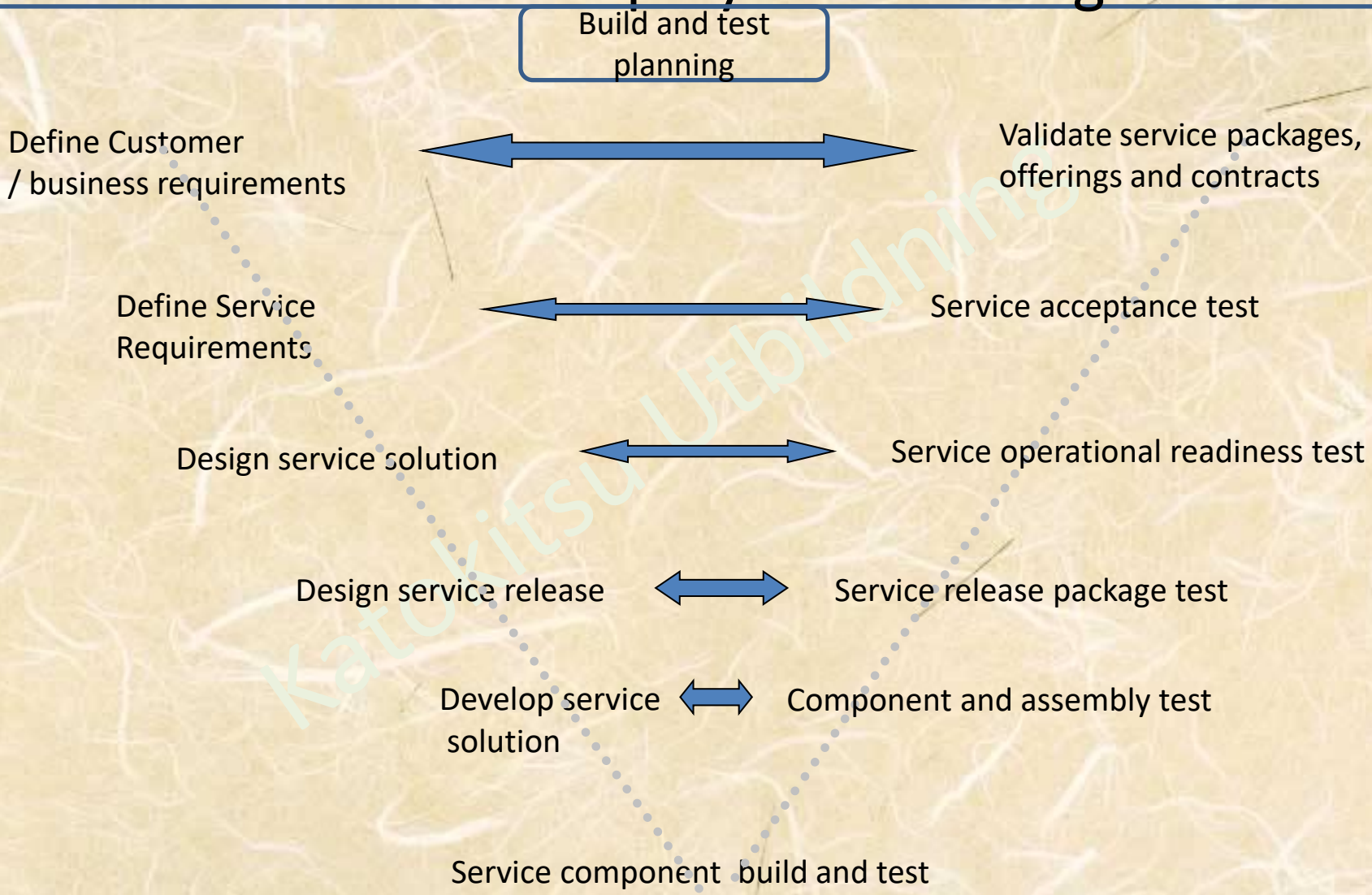
An other terminology for this is 'Test configuration management'.

Activities:

- Developing build plans from the SDP, design specifications and environment configuration requirements
- Establishing the logistics, lead times and build times to set up the environments
- Defining a configuration baseline for the build environment, to ensure that each build is carried out in a known environment
- Testing the build and related procedures
- Scheduling the build and test activities
- Assigning resources, roles and responsibilities to perform key activities, for example:
  - Security procedures and checks
  - Technical support
  - Preparing build and test environments
  - Managing test databases and test data
  - Software asset and licence management
  - Service asset and configuration management – configuration audit, build and baseline management
- Defining and agreeing the build exit and entry criteria.

V-model

Release and Deployment Management



Release and Deployment Management

Release package and build planning

Develop mechanisms, plans or procedures for the following:

- Managing stakeholder change and communications by:
  - Obtaining and maintaining the list of contacts and their details
  - Communicating the proposed changes, the expected benefits and how the change affects the organization and staff
- Training people and transferring knowledge
- Establishing that the services and service assets (e.g. agreements and contracts) are in place
- Agreeing on schedules:
  - Agreeing the delivery schedules and handling any changes/delays
  - Finalizing the logistics and delivery procedures and checklists
  - Scheduling and allocating controlled transition environments, facilities and tools for: (i) acquisition of service assets and components, and (ii) release packaging, building and testing
- Developing procedures and mechanisms using available SACM, release, content/electronic publishing and other tools to:
  - Build, copy, promote, distribute, audit, install and activate a release
  - Manage software licences, digital rights and intellectual property rights (IPR)
- Converting systems and users from the current applications and technology to the new or changed service, e.g. migrate or reformat application data and information

Release and Deployment Management

Release package and build planning

Developing the service management capability and resources for:

•Conducting site surveys
•Updating service information, e.g. service catalogue, release documentation
•Building and preparing the management systems and other operational systems, e.g. systems and event management, measurement systems
•Operating and handling the predicted capacity required for support
•Operating the controlled environments including procedures to scale up capacity if required
•Documenting and providing the information to be created and/or updated during transition, e.g. remediation plans to be issued and published
•Installing the new or changed service ready for activation
•Transferring/transitioning a service or service team or organization
•Decommissioning and/or disposing of service assets and components
•Retiring services

•Assessing the readiness of a target deployment group (customers, users and service operation functions) to take a release

•Defining and agreeing the packaging entry and exit criteria.

Release and Deployment Management

More planning…

Logistics:

How and when, leadtimes, delay effects, progress tracking, secure storage, customs, disposing, accomodation, temporary solutions, facilities

Pilot:

Parallell or seriel, politics, speed and costs, training methods, culture and language, Support

Financial:

Capital, contracts and licenses, intellectual property

Release and Deployment Management

Release and Build documentation

Asset management:

Procedures and documents for purchasing, distributing, installing, moving and controlling assets and components that are relevant to acquiring, building and testing a release.

- Contracts and agreements (e.g. for ordering new equipment or software)
- Purchase requests and ordering
- Request fulfilment
- Goods inwards and delivery
- Health and safety guidelines
- Security policies and procedures
- Leasing agreements
- Intellectual property rights/digital rights
- Support agreements

Release and Deployment Management

Release and Build documentation

Procedures / release models for:

- Managing service and infrastructure configurations
- Distributing and installing software
- Distributing, translating and converting data and information
- Delivering, installing and moving equipment
- Cleansing data and media
- Disposing of documentation, media and equipment
- Building, commissioning and decommissioning test environments, infrastructures and facilities
- Publishing knowledge, information and data
- Service validation and testing
- Change management
- Documenting licence agreements and licence headings together with ‘proof of licence’.

Release and Deployment Management

Release and Build documentation

Solution documentation includes:

- Roles and responsibilities
- Process descriptions and procedures
- Support and operations manuals, service desk scripts etc.
- Communications, training and knowledge transfer deliverables
- User manuals with work instructions
- Service information
- Business context and marketing information
- Service catalogue, SLA and supporting documentation:
  - Hardware and software information
  - Logical and physical architectural overview
  - Detailed technical descriptions and references
- Technical information
- Service management and operations plans
- IT service continuity planning details

Release and Deployment Management

Build package

Activities:

■ Assemble and integrate the release components in a controlled manner to ensure a reproducible process

■ Create the build and release documentation including:

- Build, installation and test plans, procedures and scripts
- Details of how to monitor and check the quality of the release and how to recognize and react to issues
- The automated or manual processes and procedures required to distribute, deploy and install the release into the target environment (or remove it as necessary)
- Procedures to back out release units or remediate a change should a release fail
- Procedures for tracking and managing software licences and digital rights

■ Install and verify the release package

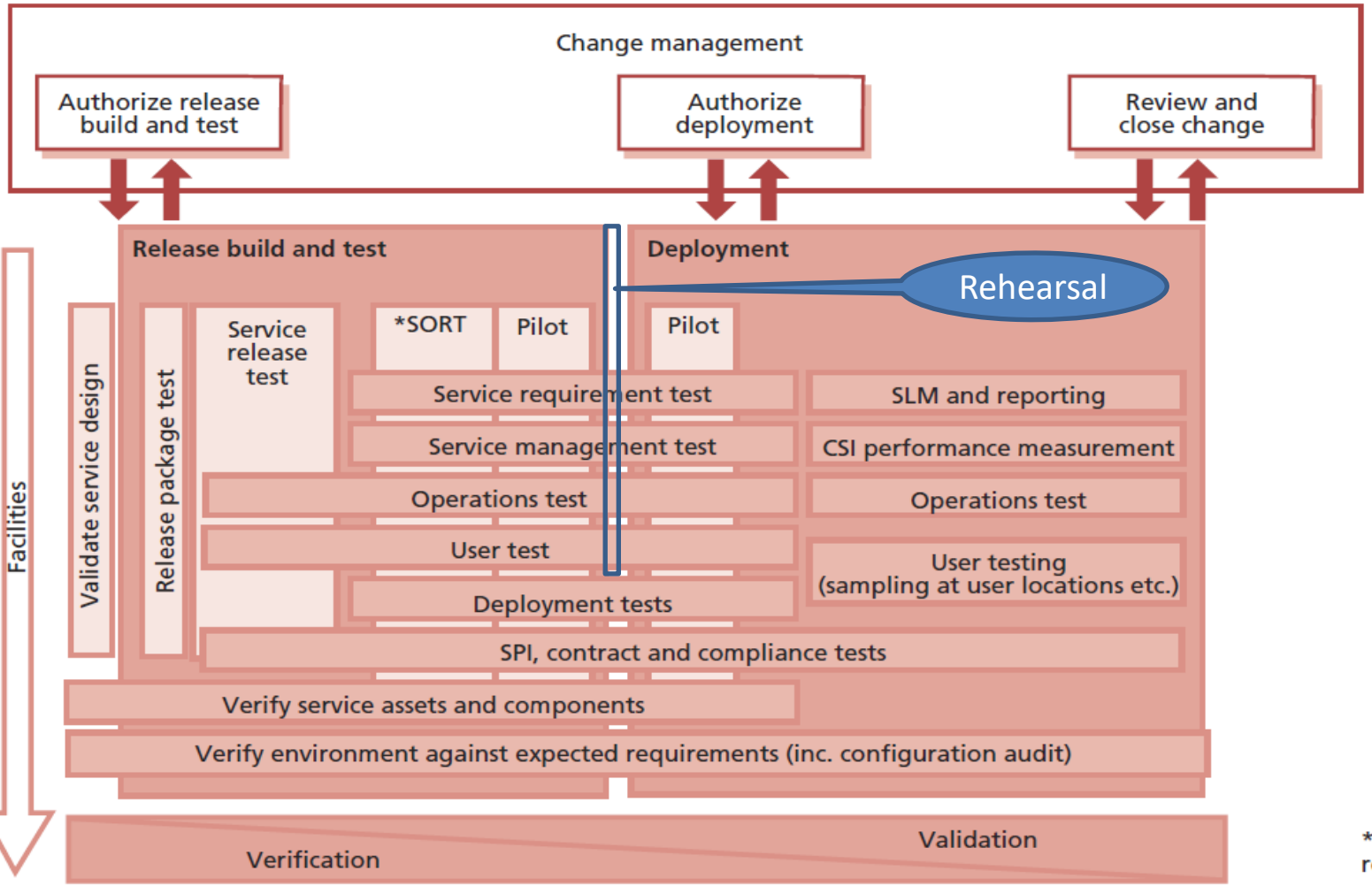
■ Baseline the contents of the release package

■ Send a service notification to inform relevant parties that the release package is available for installation and use.

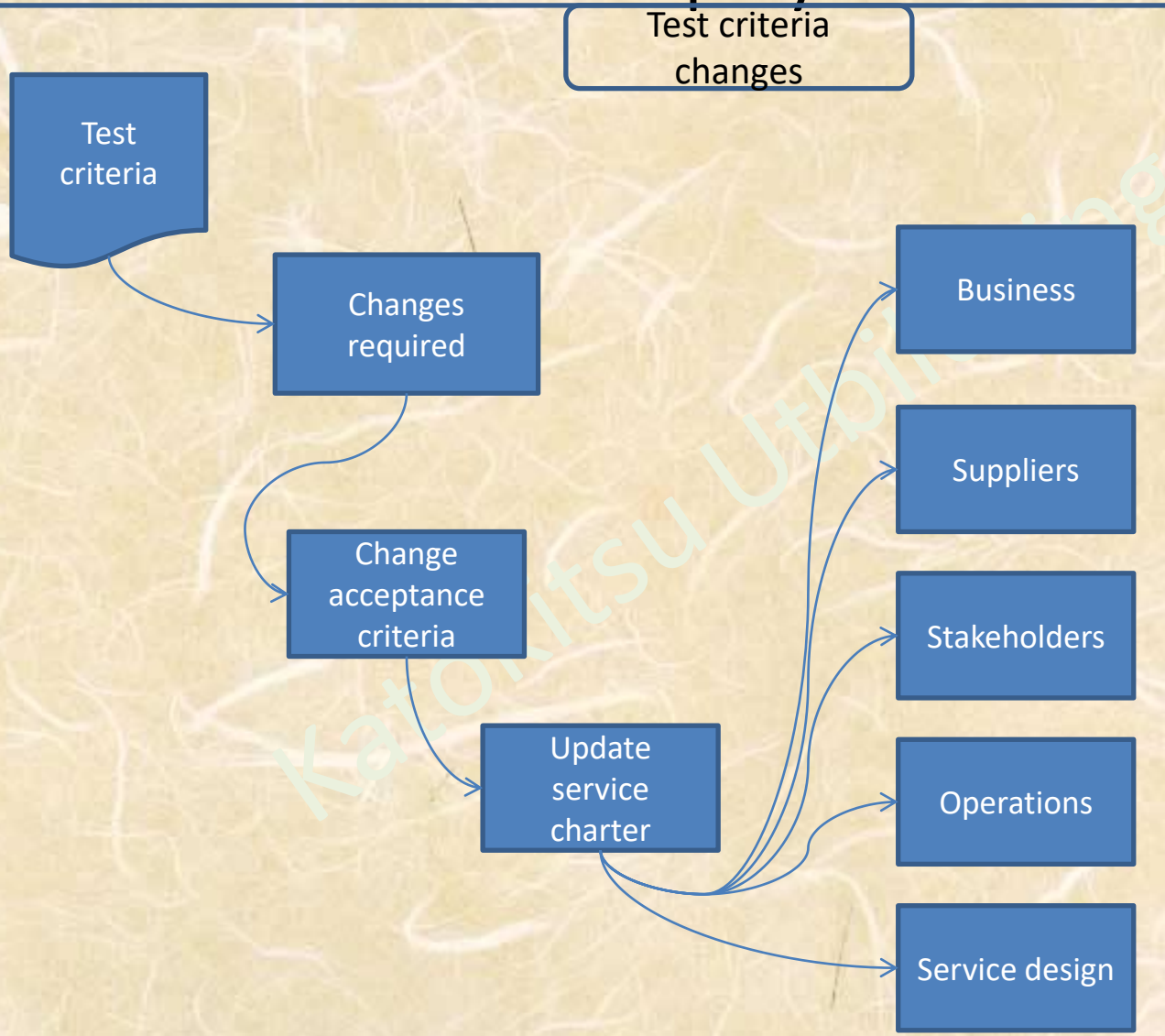
Release and Deployment Management

Test

Test



Release and Deployment Management



Release and Deployment Management

Remediation

REMEDIATE/BACK OUT RELEASE

A decision may be made to remediate the release because:

- A documented milestone is not met during the deployment
- A deployment step fails, or behaves in an unexpected manner
- Verification shows that the deployment has not succeeded.

The most common form of remediation is to back out the release, restoring all hardware, software and data to the previous baseline.

Alternative forms of remediation include implementing normal changes or emergency changes to resolve problems, or invoking IT service continuity plans to provide the service.

Release and Deployment Management

Early Life Support, ELS

During ELS, the deployment team implements improvements and resolves problems that help to stabilize the service

At agreed milestones in early life support, it is important to ***assess the issues and risks***, particularly those that impact the handover schedule and costs.

Service transition monitors the performance of the new or changed service in early life support until the ***exit criteria*** are achieved.

Release and Deployment Management

Closure

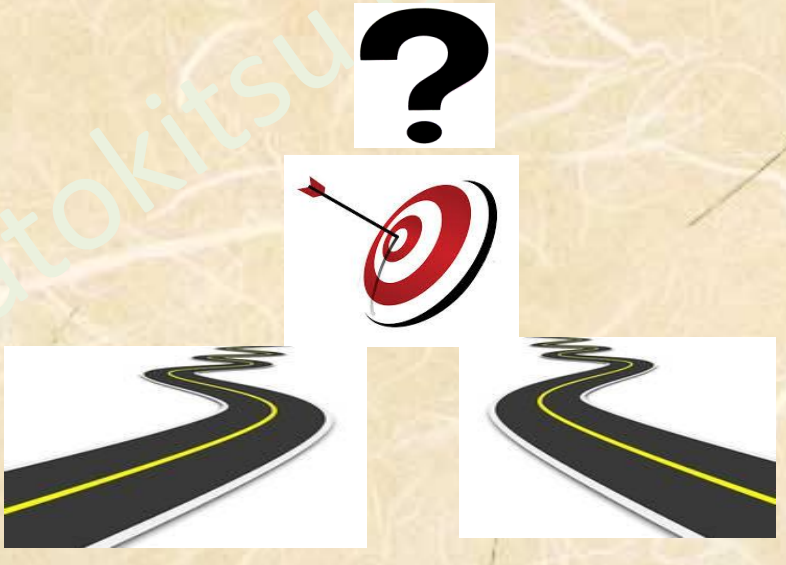
■ Capture experiences and feedback on customer, user and service provider satisfaction with the deployment
■ Highlight quality criteria that were not met.
■ Check that any actions, necessary fixes and changes are complete.
■ Review open changes and ensure that funding and responsibility for open changes are agreed before handover.
■ Review performance targets and achievements, including resource use and capacity such as user accesses, transactions and data volumes.
■ Make sure there are no capability, resource, capacity or performance issues at the end of the deployment.
■ Check that any problems, known errors and workarounds are documented and accepted by the customers/business and/or suppliers.
■ Review the risk register and identify items that impact service operation and support. Address risks or agree action such as moving the risks to the service transition risk register.
■ Check that redundant assets have been removed.
■ Check that the service is ready for transition from early life support into service operation.

Deployment is completed with a handover of the support for the deployment group or target environment to the service operation functions.

Change evaluation

Purpose

The purpose of the change evaluation process is to provide a consistent and standardized means of determining the performance of a service change in the context of likely impacts on business outcomes, and on existing and proposed services and IT infrastructure.
The actual performance of a change is assessed against its predicted performance.
Risks and issues related to the change are identified and managed.



Change evaluation

Objectives

■ Set stakeholder expectations correctly and provide effective and accurate information to change management to make sure that changes which adversely affect service capability and introduce risk are not transitioned unchecked

■ Evaluate the intended effects of a service change and as much of the unintended effects as is reasonably practical given capacity, resource and organizational constraints

■ Provide good-quality outputs so that change management can expedite an effective decision about whether or not a service change is to be authorized.

Change evaluation

Scope

The change evaluation process describes a formal evaluation that is suitable for use when significant changes are being evaluated.

Each organization must decide which changes should use this formal change evaluation, and which can be evaluated as part of the change management process.

This decision will normally be documented in change models used to manage each type of change.

Change evaluation

Value to business

Before each authorization the change should be evaluated to ensure that risks have been managed and that predicted and actual performance match the business requirements. Some organizations require a separate RFC for each of these steps; others use a documented workflow to manage all of these stages with a single change request.

The term ‘performance’ is used in change evaluation to mean the utilities and warranties for the service, which provide the ability of the service to contribute to the performance of the customer’s assets.

Change evaluation

Policies

■ Service designs or service changes will be evaluated before being transitioned.
■ Every change must be evaluated, but only significant changes will use the formal change evaluation process, criteria must be defined to identify which changes are in scope of this process.
■ Change evaluation will identify risks and issues related to the service that is being changed, and to any other services or shared infrastructure.
■ Any deviation from predicted to actual performance will be managed by the customer or customer representative by

(i) accepting the change even though actual performance is different from what was predicted,
(ii) Rejecting the change, or
(iii) Requiring a new change to be implemented with revised predicted performance agreed in advance.

No other outcomes of change evaluation are allowed.

Change evaluation

Principles

■ The unintended as well as the intended effects of a change need to be identified and their consequences understood and considered. This includes effects on other services or shared infrastructure as well as the effects on the service being changed.

■ A service change will be fairly, consistently, openly and, wherever possible, objectively evaluated.

■ An evaluation report, or interim evaluation report, will be provided to change management to facilitate decision-making at each point at which authorization is required.

Change evaluation

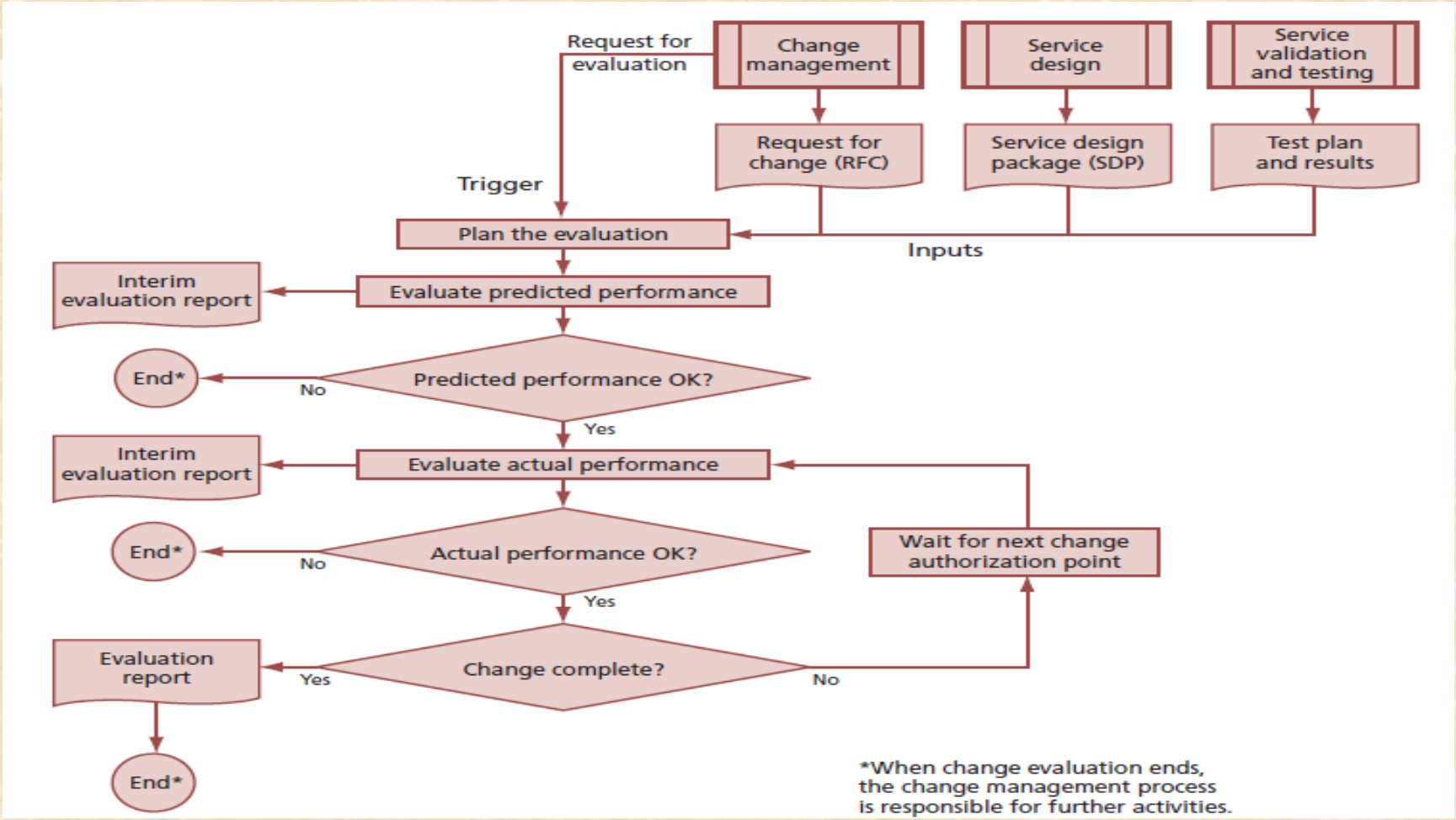
Basic concepts

The change evaluation process uses the Plan–Do–Check–Act (PDCA) model to ensure consistency across all evaluations.

Each evaluation is planned and then carried out in multiple stages, the results of the evaluation are checked and actions are taken to resolve any issues found.

Change evaluation

Process



Change evaluation

Terminology

Term	Meaning
Actual performance	The performance achieved following a service change.
Countermeasure	The mitigation that is implemented to reduce risk.
Deviations report	A report of the difference between predicted and actual performance
Evaluation report	A report generated by the change evaluation process, which is passed to change management and which comprises: ■ A risk profile ■ A deviations report ■ A recommendation ■ A qualification statement.
Performance	The utilities and warranties of a service.
Performance model	A representation of a service that is used to help predict performance.
Predicted performance	The expected performance of a service following a service change
Residual risk	The remaining risk after countermeasures have been deployed

Change evaluation

Terminology, cont

Term	Meaning
Service capability	The ability of a service to perform as required
Service change	A change to an existing service or the introduction of a new service
Test plan and results	The test plan is a response to an impact assessment of the proposed service change. Typically the plan will specify how the change will be tested; what records will result from testing and where they will be stored; who will authorize the change; and how it will be ensured that the change and the service(s) it affects will remain stable over time. The test plan may include a qualification plan and a validation plan if the change affects a regulated environment. The results represent the actual performance following implementation of the change.

Change evaluation

Evaluation report

■ **Risk profile**
A representation of the residual risk left after a change has been implemented and after countermeasures have been applied.

■ **Deviations**
The difference between predicted and actual performance following the implementation of a change.

■ **A qualification statement (if appropriate)**
Following review of qualification test results and the qualification plan, a statement of whether or not the change has left the service in a state whereby it could not be qualified. The qualification statement formally states that the IT infrastructure is appropriate and correctly configured to support the specific application or IT service.

■ **A validation statement (if appropriate)**
Following review of validation test results and the validation plan, a statement of whether or not the change has left the service in a state whereby it could not be validated. The validation statement formally states that the new or changed service or application meets a documented set of requirements.

■ **A recommendation Based on the other factors** within the evaluation report, a recommendation to change

Change evaluation

Triggers, inputs, outputs

The trigger for change evaluation is receipt of a request for evaluation from change management.

Inputs:

- SDP
- Change proposal
- RFC, change record and detailed change documentation
- Discussions with stakeholders
- Test results and report.

Outputs:

- Interim evaluation report(s) for change management
- Evaluation report for change management.

Change evaluation

Interfaces

Transition planning	Ensure that appropriate resources are available when needed and that each service transition is well managed.
Change Management	Which types of change will be subject to formal evaluation, and the time required for this evaluation must be included in the overall planning for the change. Change management provides the trigger for change evaluation, and the evaluation report must be delivered to change management in time for the CAB (or other change authority) to use it to assist in their decision-making.
Service Design	Change evaluation requires information about the service, which is supplied by service design coordination in the form of a service design package
Service Level Management	Ensure full understanding of the impact of any issues identified, and obtain use of user or customer resources if these are needed to help perform the evaluation
Service Validation and testing	Coordinate activities with this process to ensure that required inputs are available in sufficient time.

Change evaluation

Information management

Much of the information required for change evaluation should be available from the SKMS.

All evaluation reports should be checked in to the CMS and softcopy versions of the reports should be stored in the SKMS.

Change evaluation

Critical Success Factors

Critical Success Factor	KPI
Stakeholders have a good understanding of the expected performance of new and changed Services	● **Reduced number of incidents for new** or changed services due to failure to deliver expected utility or warranty ● **Increased stakeholder satisfaction with** new or changed services as measured in customer surveys
Change management has good quality evaluations to help them make correct decisions	● **Increased percentage of evaluations** delivered by agreed times ● **Reduced number of changes that have** to be backed out due to unexpected errors or failures ● **Reduced number of failed changes** ● **Increased change management** personnel satisfaction with the change evaluation process as measured in regular surveys.

Change evaluation

Challenges

- Developing standard performance measures and measurement methods across projects and suppliers
- Understanding the different stakeholder perspectives that underpin effective risk management for the change evaluation activities
- Understanding, and being able to assess, the balance between managing risk and taking risks as this affects the overall strategy of the organization and service delivery
- Measuring and demonstrating less variation in predictions during and after transition
- Taking a pragmatic and measured approach to risk
- Communicating the organization's attitude to risk and approach to risk management effectively during risk evaluation
- Building a thorough understanding of risks that have impacted or may impact successful service transition of services and releases
- Encouraging a risk management culture where people share information.

Change evaluation

Risks

■ Lack of clear criteria for when change evaluation should be used

■ Unrealistic expectations of the time required for change evaluation

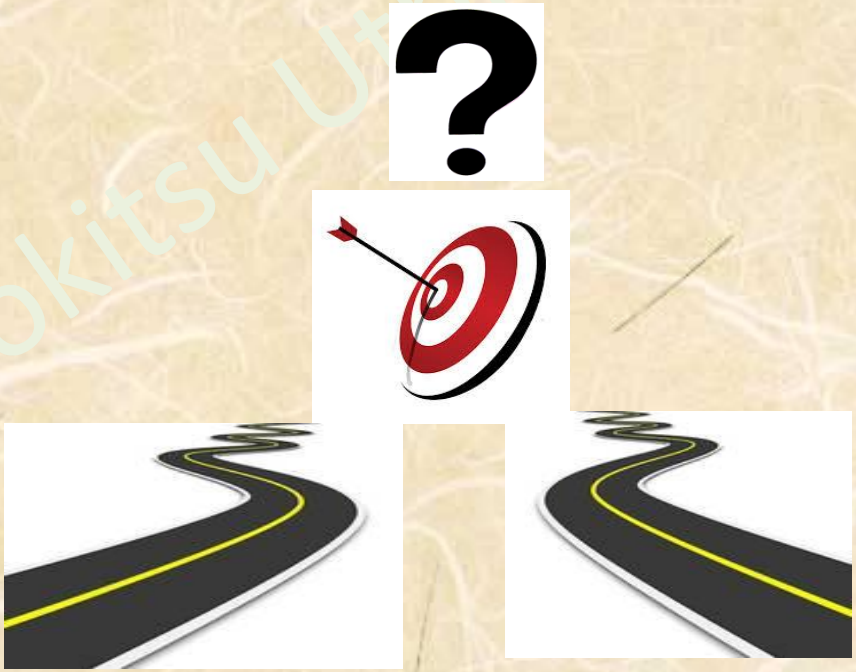
■ Change evaluation personnel with insufficient experience or organizational authority to be able to influence change authorities

■ Projects and suppliers estimating delivery dates inaccurately and causing delays in scheduling change evaluation activities.

Knowledge Management

Purpose

Purpose:
To share perspectives, ideas, experience and information; to ensure that these are available in the right place at the right time to enable informed decisions; and to improve efficiency by reducing the need to rediscover knowledge.



Knowledge Management

Objectives

Decision making	Improve the quality of management decision making by ensuring that reliable and secure knowledge, information and data is available throughout the service lifecycle
Efficiency and quality	Enable the service provider to be more efficient and improve quality of service, increase satisfaction and reduce the cost of service by reducing the need to rediscover knowledge
Customer benefits	Ensure that staff have a clear and common understanding of the value that their services provide to customers and the ways in which benefits are realized from the use of those Services
Controlled access	Maintain a service knowledge management system (SKMS) that provides controlled access to knowledge, information and data that is appropriate for each audience
Use and maintain	Gather, analyse, store, share, use and maintain knowledge, information and data throughout the service provider organization.

Knowledge Management

Scope

Knowledge management includes oversight of the management of knowledge, the information and data from which that knowledge derives

Knowledge Management

Value to business

$ The ability to deliver a quality service or process rests to a significant extent on the ability of those involved to respond to circumstances

– and that in turn rests heavily on their understanding of the situation, the options and the consequences and benefits, i.e. their knowledge of the situation in which they are currently, or in which they may find themselves.

$ The quality and relevance of Knowledge rests on the accessibility, quality and continued relevance of the underpinning data and information available to service staff.

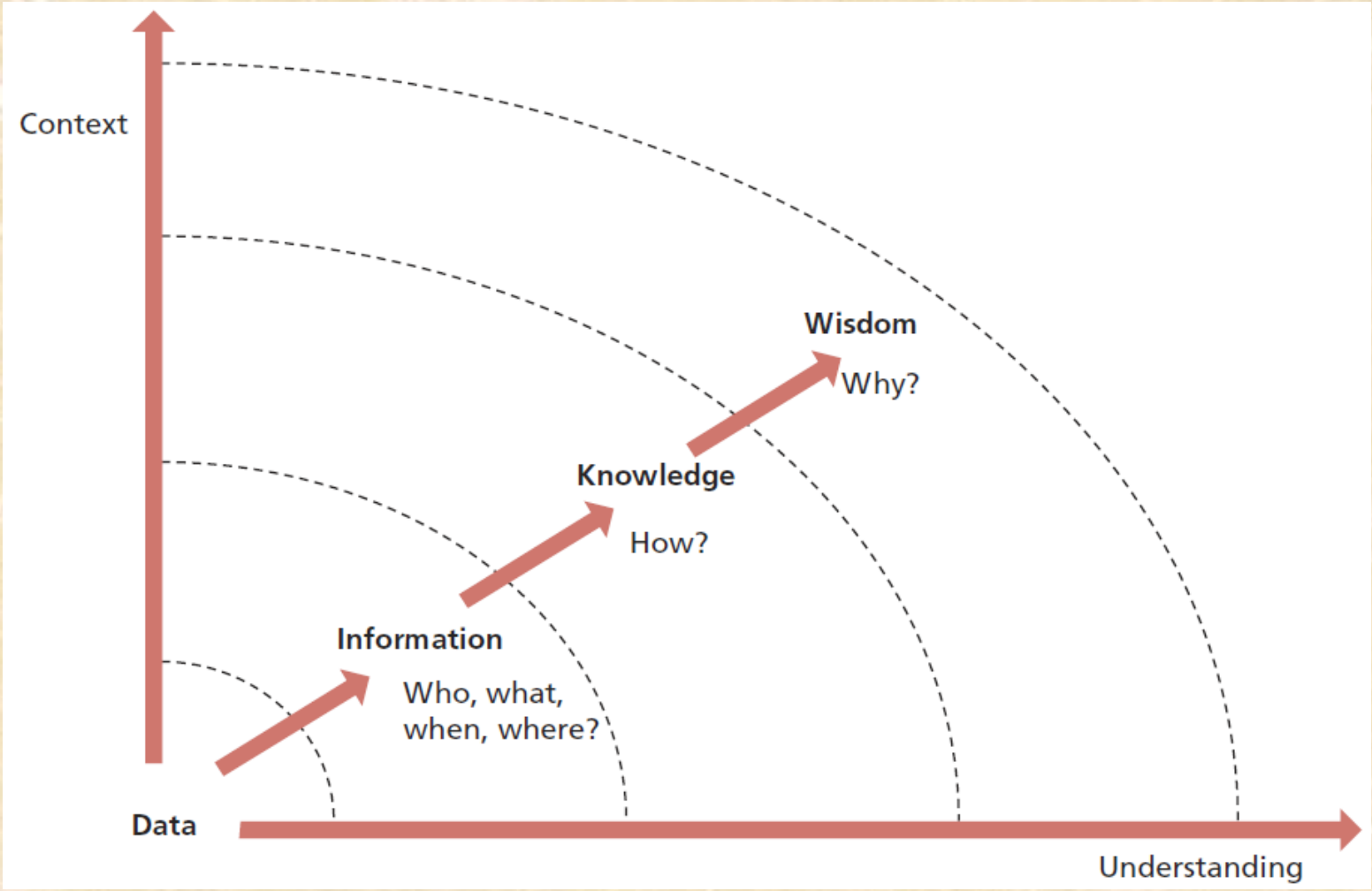
Knowledge Management

Policies

- Knowledge and information needed to support the services will be stored in a way that allows them to be accessed by all staff when and where they are needed.
- All policies, plans and processes must be reviewed at least once per year.
- All knowledge and information should be created, reviewed, approved, maintained, controlled and disposed of following a formal documented process.

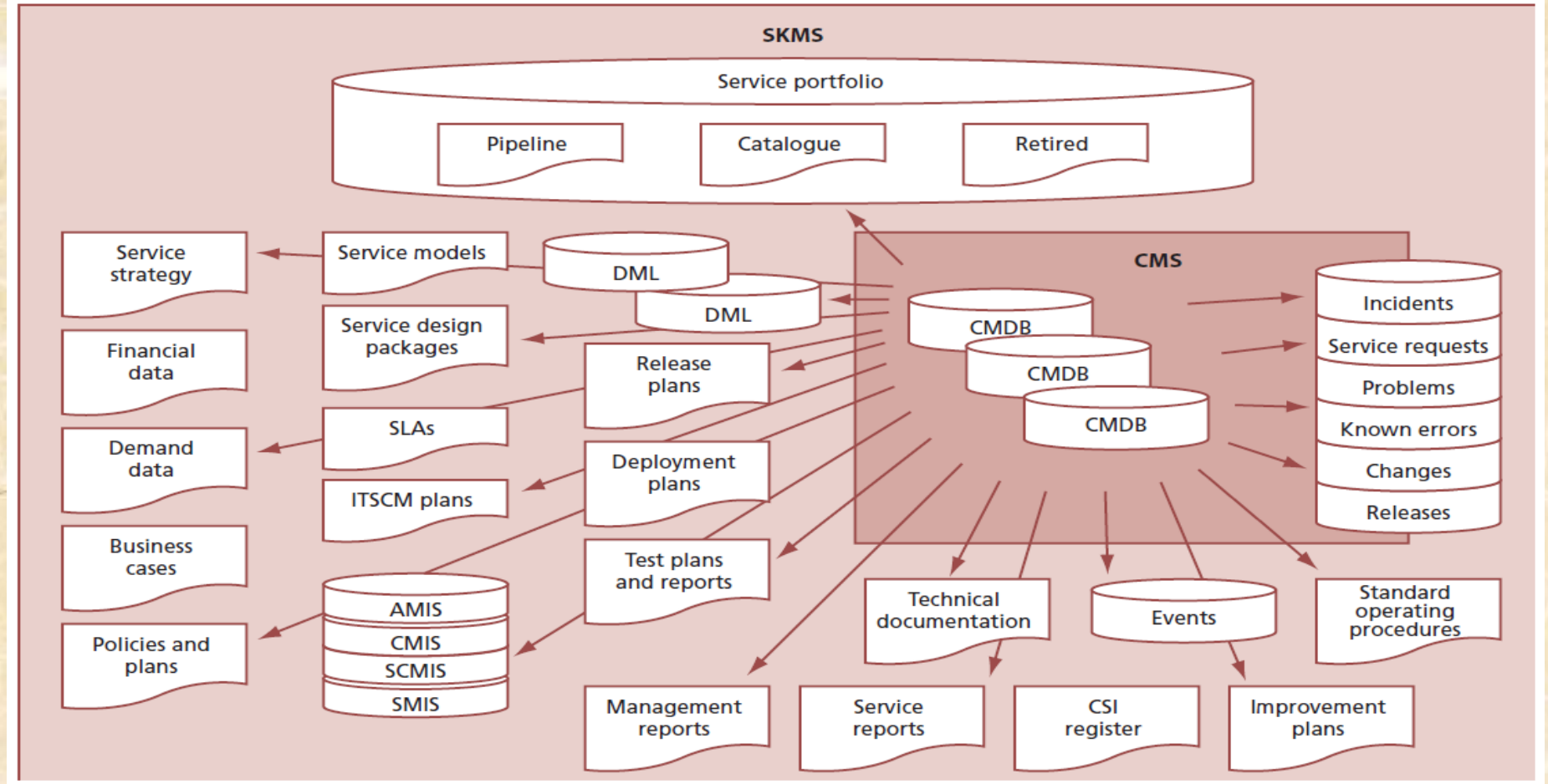
Knowledge Management

Principles, basic concepts



Knowledge Management

SKMS



Knowledge Management

Considerations

- What knowledge is necessary
- What data is available
- Cost of capturing and maintaining data
- Intellectual property rights
- Standard form and content structure
- Data protection, privacy, security, ownership, rights of access
- Availability at the right time
- Change process

Organizing for Service Transition

Small organisation

Small organisation :

The service transition manager is the process owner, process manager and process practitioner for transition planning and support

The change, configuration and release (CCR) manager is the process owner and the process manager for change management, service asset and configuration management (SACM), release and deployment management, and knowledge management.

The evaluation and test manager is the process owner and the process manager for change evaluation and for service validation and test

Organising for Service Transition

Large organisation

Large organisation :

Central organisation includes all process owners , change management and release and deployment teams, SACM team, knowledge manager. Possibly, there are different teams per product /service area.

Organising for Service Transition

Functions

Function:
Specific organisational unit for executing specific tasks, e.g. Service Desk, Network team, Server Team, Release and Deployment team, ….

In larger organisations, even several departments may execute a given function, while in smaller organisations a team can execute several functions.

Organising for Service Transition

Roles

Roles:

A role is a set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process or function.

Technical and application management provide the technical resources and expertise to manage the whole service lifecycle, and practitioner roles within service transition may be performed by members of these functions.

Organising for Service Transition

Roles – Service Owner

The service owner is accountable for the delivery of a specific IT service.

The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and accountable to the IT director or service management director for the delivery of the service.

The service owner's accountability for a specific service within an organization is independent of where the underpinning technology components, processes or professional capabilities reside.

The service owner is responsible for continual improvement and the management of change affecting the service under their care. The service owner is a primary stakeholder in all of the underlying IT processes which enable or support the service they own.

Organizing for Service Transition

Roles – Change Management

Process owner:

- Carrying out the generic process owner role for the change management process
- Designing change authority hierarchy and criteria for allocating RFCs to change authorities
- Designing change models and workflows
- Working with other process owners to ensure that there is an integrated approach to the design and implementation of change management, service asset and configuration management, release and deployment management, and service validation and testing

Process manager:

- Carrying out the generic process manager role for the change management process
- Planning and managing support for change management tools and processes
- Maintaining the change schedule and projected service outage
- Coordinating interfaces between change management and other processes – especially service asset and configuration management and release and deployment management.

Organizing for Service Transition

Roles – Change Management

Initiator:

- Identifying the requirement for a change
- Completing and submitting a change proposal or / and if appropriate
- Attending CAB meetings to provide further information about the RFC or change proposal if invited
- Reviewing change when requested by change management, and specifically before closure.

Practitioner:

- Verifying that RFCs are correctly completed
- Allocating RFCs to appropriate change authorities based on defined criteria
- Submitting requests for evaluation to trigger the change evaluation process
- Formally communicating decisions of change authorities to affected parties
- Monitoring and reviewing activities of teams and functions that build and test changes to ensure that the work is carried out correctly.
- Publishing the change schedule and projected service outage and ensuring that they are available when and where needed.

Authority / CAB:

In many organizations, the CAB is the change authority for some categories of change. In other organizations the CAB is just an advisory body.

Organizing for Service Transition

Roles - SACM

Process owner:
■ Carrying out the generic process owner role for the SACM process
■ Agreeing and documenting the scope for SACM, including the policy for determining which service assets should be treated as configuration items
■ Working with other process owners to ensure there is an integrated approach to the design and implementation of SACM, change management, release and deployment management, and knowledge management.

Process Manager:
■ Carrying out the generic process manager role for the SACM process
■ Accountable to the organization for stewardship of fixed assets of the organization that are under the control of IT
■ Defining and agreeing the service assets that will be treated as configuration items
■ Ensuring that configuration data is available when and where it is needed to support other service management processes
■ Planning and managing support for SACM tools and processes
■ Coordinating interfaces between SACM and other processes, especially change management, release and deployment management, and knowledge management.

Configuration analyst:

Organising for Service Transition

Roles - SACM

Configuration analyst:

- Proposing scope for service asset and configuration management
- Supporting the process owner and process manager in the creation of principles, processes and procedures
- Defining the structure of the configuration management system, including CI types, naming conventions, required and optional attributes and relationships
- Training staff in SACM principles, processes and procedures
- Performing configuration audits.

Librarian:

- Controlling the receipt, identification, storage and withdrawal of all supported CIs
- Maintaining status information on CIs and providing this as appropriate
- Archiving superseded CIs
- Assisting in conducting configuration audits
- Identifying, recording, storing and distributing issues relating to service asset and configuration management.

Organizing for Service Transition

Roles – Release and Deployment

Process owner:

■ Carrying out the generic process owner role for the release and deployment management process
■ Designing release models and workflows
■ Working with other process owners to ensure there is an integrated approach to the design and implementation of change management, service asset and configuration management, release and deployment management, and service validation and testing.

Process manager:
■ Carrying out the generic process manager role for the release and deployment management process
■ Planning and coordinating all resources needed to build, test and deploy each release, including resources from other functions such as technical management or application management
■ Planning and managing support for release and deployment management tools and processes
■ Ensuring that change authorization is provided before any activity that requires this, for example before a release is checked in to the definitive media library (DML) and before it is deployed to a live environment
■ Coordinating interfaces between release and deployment management and other processes, especially change management, SACM, and service validation and testing.

Managing people

Organisational change

KEY activities that are required to manage the organizational change.

• A project team is created

• The stakeholder map and communication plan are developed quickly to be sympathetic to the sense of urgency and to demonstrate an organized, responsive plan is being created to assist the organizational comfort level of the proposed change

• Workshops are held and include key elements, chief information officer (CIO) support and users who are negatively impacted by the change. CIO presence is a crucial element in showing executive support for the change, as is the inclusion of negatively impacted users to bring them into the team as early as possible to build the solution

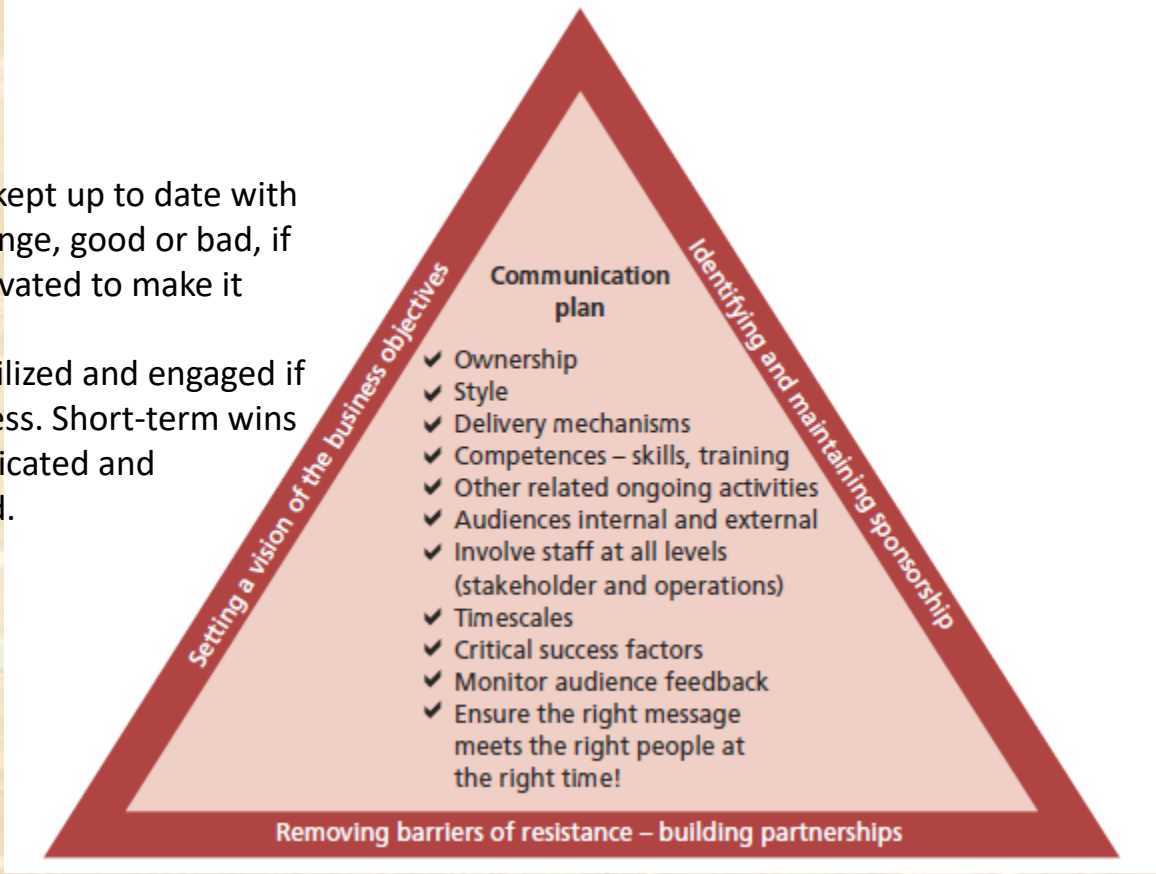
• Training is matched to those with an appropriate need and not just a blanket approach, and is not restricted to IT staff only

Managing people

Communication

Strategy

People need to be kept up to date with the progress of change, good or bad, if they are to be motivated to make it happen.
People will be mobilized and engaged if they can see progress. Short-term wins should be communicated and progress celebrated.



Managing people

Methods

- Workshops
- Newsletters
- Training sessions
- Meetings on different levels
- Floorwalks
- Q&A Feedback postings
- Intranet
- Simulation games
- Posters
- Small reference cards

… understand the effect that current culture may have as a ‘barrier’ to realizing change....

Managing people

Sample artifacts to use and produce

- Stakeholder map
- Current organization and capability assessment
- Current and required competency model and competency assessments
- Constraints (including organization, capability, resources)
- Service management process model
- Policies, processes and procedures
- Roles and responsibility definitions, e.g. a RACI
- Relationship management
- Communication plan
- Supplier framework, especially where multiple suppliers are involved.

Managing people

RACI

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

Managing people

Cultural aspects

Language, communication, knowledge flow, communities, networks, working environments, history, meetings, rewards and motivations, time

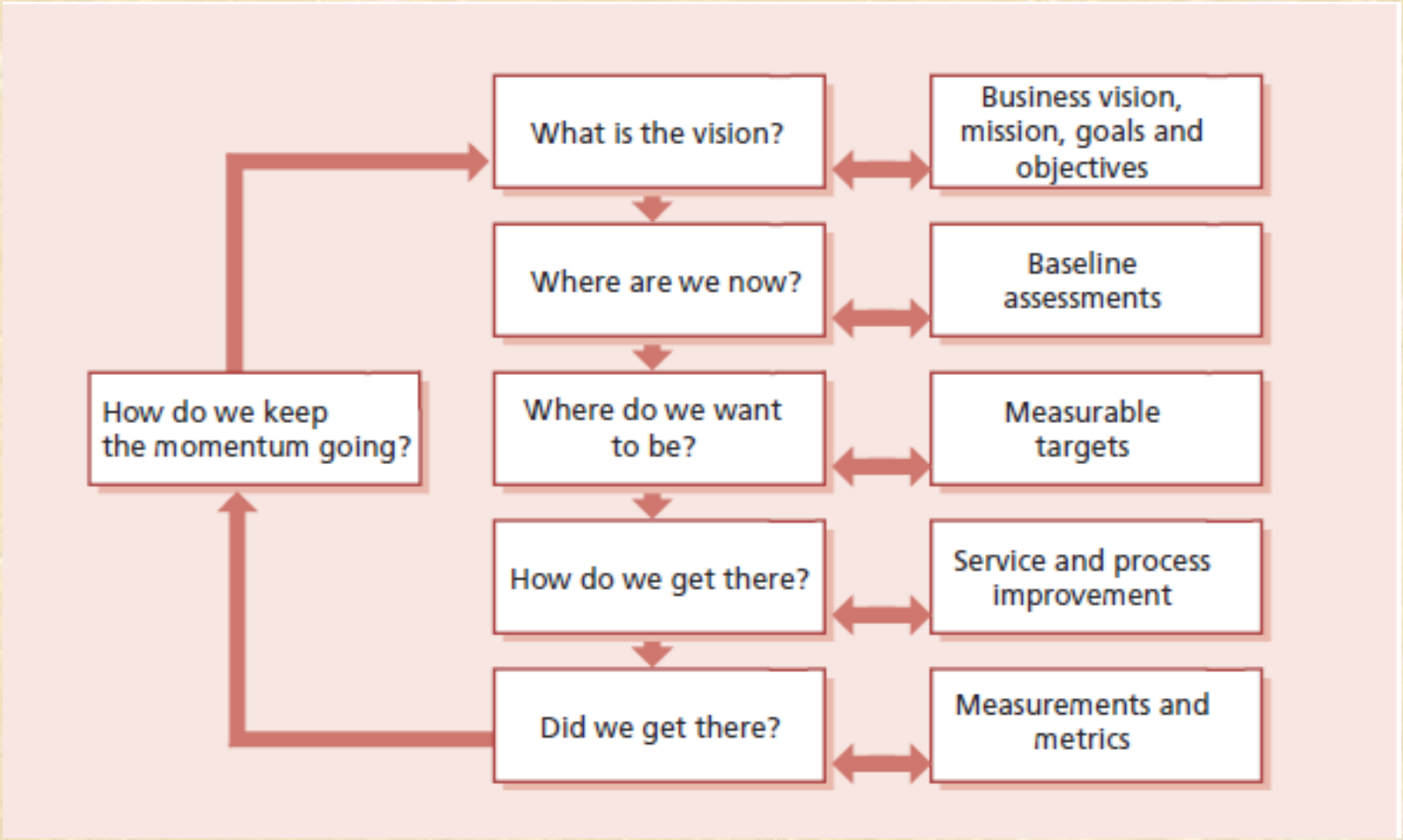
… understand the effect that current culture may have as a ‘barrier’ to realizing change....

Technology considerations

Green IT	Workflow tools	Build and release tools
SKMS/CMS/CMDB	Data mining	Community portals
Enterprise wide	Data extract, load, transfer	Presentation tools
Transition targeted	Document management	Flow charting
ITSM tools	Database management	Brainstorm
System tools	Discovery, audit	
Measurement, Reporting	Graphical mapping	
Collaborative tools (shared calendars, Lync…)	Distribution, Installation, deinstallation	

Implementing and improving Service Transition

Steps



Implementing and improving Service Transition

Designing

Area	Example
Standards and policies, legistlation	Visibility, SOX, Independence
Relationships	HR, Facilities ,Telecom, Production, Education
Programme and Project management	Transition strategy, PRINCE2
Development teams and suppliers	Errors during test and pilot, Early Life Support
Customers, users	Communication
Budget and resources	Founding, Human resources, Test environment, Network resources
Risk and value	Measurable satisfaction and benefits, cost control

Critical Success Factors

Challenges

- Large stakeholder and customer group
- Many contacts, interfaces and relationships
- Inherent differences among the legacy systems, new technology and human elements
- Stability – flexibility
- Creating an environment that fosters standardization, simplification and knowledge sharing
- Developing standard performance measures and measurement methods across projects and suppliers

Critical Success Factors

Critical Success Factors

Manage the challenges (see prev. slide)

Additionally:

- Creating and maintaining new and updated knowledge in a form that people can find and use
- Developing good-quality systems, tools, processes and procedures required to manage a service transition practice
- Good service management and IT infrastructure tools and technology
- Being able to appreciate and exploit the cultural and political environment
- Being able to understand the service and technical configurations and their dependencies

Critical Success Factors

Risks and difficulties

■ Change in accountabilities, responsibilities and practices of existing projects that de-motivate the workforce
■ Alienation of some key support and operations staff
■ Additional unplanned costs to services in transition
■ Resistance to change and circumvention of the processes due to perceived bureaucracy.

■ Short timescale
- In time-critical situations, implementation of a new or changed service may be more important than a degree of disruption. This is effectively a risk management decision

■ Restricted finances
■ Restricted resource availability – not enough people or lack of test environments, inadequate tools etc.
■ Absence of anticipated skill sets
■ Internal political difficulty
■ Difficult customers
- e.g. do not make staff and resources available to facilitate effective service transition,

Certification focus

Change Management process

Develop a change management process that will be implemented across the entire IT organization and, in order to address the specific issues, ensure that the process includes:

- A range of different change models to handle each different type of change
- A change authorization matrix indicating sign-off levels for the various types of change
- A risk model to be used by all of IT to support the assessment and evaluation activities

Focus on the need to develop a change management process that provides both effectiveness in assessing, evaluating and authorizing different types of changes, as well as efficiencies in handling the change volume. A relevant change management process also has to allow for appropriate levels of risk, and must allow low-risk changes to proceed with minimal bureaucracy to allow available resources to be concentrated where they will deliver the maximum benefit.

The change authorization matrix will allow changes to be authorized at the appropriate levels, speeding up lower risk and routine change but ensuring appropriate attention is paid to potentially more dangerous changes. The risk model will be used across the organization, and help ensure that the right changes are dealt with at the right levels. Risk needs to reflect also on business, not only on IT.

Too much bureaucracy will result in no change or circumventing the process.