

ITIL Release, Control and Validation

Contents

1 Introduction to service management.....	8
1.1 Best practice	8
1.2 The ITIL frame work.....	8
1.3 Service management.....	8
1.4 Processes and functions.....	9
1.5 Roles	9
1.5.1 Process owner	9
1.5.2 Process manager	10
1.5.3 Process practitioner	10
1.5.4 Service owner.....	10
1.5.5 The RACI model	11
1.6 Release, control and validation supporting the service lifecycle	11
1.6.1 Purpose and objectives	11
1.6.2 Scope	11
1.6.3 Value to business of service transition activities	12
1.6.4 Transition strategy	12
1.6.5 Service transition lifecycle stages	12
1.6.6 Preparing for service transition.....	13
1.6.7 Planning and coordinating service transition.....	13
1.6.8 Provide service transition support	14
1.6.9 Processes within service transition	14
2 Change management	16
2.1 Purpose and objectives	16
2.2 Scope	16
2.3 Value to the business	16
2.4 Policies, principles and basic concepts.....	16
2.4.1 Types of change request	17
2.5 Process activities, methods and techniques	18

2.5.1 Create and record the request for change.....	18
2.5.2 Review request for change.....	18
2.5.3 Assess and evaluate change.....	18
2.5.4 Authorize change	18
2.5.5 Coordinate change implementation	19
2.5.6 Review and close change record	19
2.6 Managing organization and stakeholder change	19
2.7 Triggers, inputs, outputs and interfaces	20
2.8 Critical success factors and key performance indicators	21
2.9 Challenges and risks	22
2.10 Typical day-to-day activities performed by service operation.....	22
2.11 Roles and responsibilities.....	22
2.11.1 Change management process owner.....	22
2.11.2 Change management process manager.....	23
2.11.3 Change initiator	23
2.11.4 Change practitioner.....	23
2.11.5 Change authority.....	24
3 Service asset and configuration management.....	25
3.1 Purpose and objectives	25
3.2 Scope	25
3.3 Value to the business	25
3.4 Policies, principles and basic concepts.....	25
3.4.1 The configuration model.....	26
3.4.2 Configuration items.....	26
3.4.3 The configuration management system	26
3.5 Process activities, methods and techniques	27
3.5.1 Management and planning	27
3.5.2 Configuration identification	27
3.5.3 Configuration control	28
3.5.4 Status accounting and reporting.....	28
3.5.5 Verification and audit.....	28
3.6 Asset management.....	28

3.7 Triggers, inputs, outputs and interfaces	28
3.8 Information management	29
3.9 Critical success factors and key performance indicators	29
3.10 Challenges and risks	29
3.11 Typical day-to-day activities performed by service operation	30
3.12 Roles and responsibilities	30
3.12.1 SACM process owner	30
3.12.2 SACM process manager	30
3.12.3 Configuration analyst	31
3.12.4 Configuration librarian	31
4 Service validation and testing	32
4.1 Purpose and objectives	32
4.2 Scope	32
4.3 Value to the business	33
4.4 Policies, principles and basic concepts	33
4.4.1 Service quality policy	33
4.4.2 Risk policy	33
4.4.3 Release policy	33
4.4.4 Change management policy	33
4.4.5 Test models	33
4.4.6 Validation and testing perspectives	33
4.4.7 Business user and customer perspective	34
4.4.8 User testing – application, system and service	34
4.4.9 Operations and service improvement perspective	34
4.4.10 Levels of testing and testing models	34
4.5 Process activities, methods and techniques	35
4.5.1 Validation and test management	35
4.5.2 Plan and design tests	35
4.5.3 Verify test plan and test designs	35
4.5.4 Prepare test environment	35
4.5.5 Perform tests	35
4.5.6 Evaluate exit criteria and report	35

4.5.7 Test clean-up and closure	36
4.6 Triggers, inputs, outputs and interfaces	36
4.7 Information management	36
4.8 Critical success factors and key performance indicators	37
4.9 Challenges and risks	37
4.10 Roles and responsibilities	37
4.10.1 Service validation and testing process owner	37
4.10.2 Service validation and testing process manager	38
4.10.3 Service validation and testing practitioner	38
5 Release and deployment management	39
5.1 Purpose and objectives	39
5.2 Scope	39
5.3 Value to the business	39
5.4 Policies, principles and basic concepts	39
5.4.1 Release unit and release package	39
5.4.2 Deployment options	40
5.5 Process activities, methods and techniques	40
5.5.1 Planning	40
5.5.2 Preparation for build, test and deployment	42
5.5.3 Build and test	42
5.5.4 Service testing and pilots	42
5.5.5 Plan and prepare for deployment, and perform transfer, deployment and retirement	43
5.5.6 Verify deployment	43
5.5.7 Early life support	43
5.5.8 Review and close deployment, review and close service transition	43
5.6 Triggers, inputs, outputs and interfaces	43
5.7 Information management	44
5.8 Critical success factors and key performance indicators	44
5.9 Challenges and risks	45
5.10 Typical day-to-day activities performed by service operation	45
5.11 Roles and responsibilities	45
5.11.1 Release and deployment management process owner	45

5.11.2 Release and deployment manager	46
5.11.3 Release packaging and build practitioner	46
5.11.4 Deployment practitioner	46
5.11.5 Early life support practitioner	46
6 Request fulfilment.....	47
6.1 Purpose and objectives	47
6.2 Scope	47
6.3 Value to the business and service lifecycle	47
6.4 Policies, principles and basic concepts.....	47
6.4.1 Request models	48
6.4.2 Menu selection.....	48
6.4.3 Request status tracking	48
6.4.4 Financial approval	48
6.4.5 Coordination of fulfilment activities	48
6.5 Process activities, methods and techniques	48
6.5.1 Request receipt, logging and validation	48
6.5.2 Request categorization and prioritization.....	48
6.5.3 Request authorization	49
6.5.4 Request review	49
6.5.5 Request model execution.....	49
6.5.6 Request closure	49
6.6 Triggers, inputs, outputs and interfaces	49
6.7 Information management	50
6.8 Critical success factors and key performance indicators	50
6.9 Challenges and risks	51
6.10 Roles and responsibilities.....	51
6.10.1 Request fulfilment process owner	51
6.10.2 Request fulfilment process manager	52
6.10.3 Request fulfilment analyst	52
7 Change evaluation.....	53
7.1 Purpose and objectives	53
7.2 Scope	53

7.3 Value to the business	53
7.4 Policies, principles and basic concepts.....	53
7.5 Process activities, methods and techniques	54
7.5.1 Evaluation plan.....	54
7.5.2 Understanding intended and unintended effects of a change	54
7.5.3 Evaluation of predicted and actual performance	54
7.6 Triggers, inputs, outputs and interfaces	54
7.7 Information management.....	55
7.8 Critical success factors and key performance indicators	55
7.9 Challenges and risks	55
7.10 Roles and responsibilities.....	56
7.10.1 Change evaluation process owner	56
7.10.2 Change evaluation process manager	56
7.10.3 Change evaluation practitioner.....	56
8 Knowledge management	57
8.1 Purpose and objectives	57
8.2 Scope	57
8.3 Value to the business	57
8.4 Policies, principles and basic concepts.....	57
8.4.1 Knowledge management policies	57
8.4.2 Data-to-Information-to-Knowledge-to-Wisdom structure	58
8.4.3 The service knowledge management system	58
8.5 Process activities, methods and techniques	58
8.5.1 Knowledge management strategy	58
8.5.2 Knowledge transfer	58
8.5.3 Managing data, information and knowledge.....	59
8.6 Triggers, inputs, outputs and interfaces	59
8.7 Information management.....	60
8.8 Critical success factors and key performance indicators	60
8.9 Challenges and risks	60
8.10 Relationship with continual service improvement	60
8.11 Roles and responsibilities.....	60

8.11.1 Knowledge management process owner	60
8.11.2 Knowledge management process manager	61
8.11.3 Knowledge management process practitioner	61
8.11.4 Knowledge creator	61
9 Technology and implementation	62
9.1 Generic requirements for IT service management technology	62
9.2 Evaluation criteria for technology and tools	62
9.3 Practices for process implementation	63
9.3.1 Managing change in service operation	63
9.3.2 Service operation and project management	63
9.3.3 Assessing and managing risk in service operation	63
9.3.4 Operational staff in service design and transition	63
9.4 Challenges, critical success factors and risks relating to implementing practices and processes	64
9.4.1 Challenges	64
9.4.2 Critical success factors	64
9.4.3 Risks	65
9.5 Planning and implementing service management technologies	65
9.6 Technology for implementing collaboration, configuration management and knowledge management	65
9.6.1 Collaboration	65
9.6.2 Configuration management system	66
9.6.3 Knowledge management tools	66
9.7 The Deming Cycle	67

1 Introduction to service management

1.1 Best practice

Organizations operating in dynamic environments need to improve their performance and maintain competitive advantage. Adopting best practices in industry-wide use can help to improve capability. Sources:

- Public frameworks and standards
- Proprietary knowledge of organizations and individuals

1.2 The ITIL frame work

- Vendor-neutral
- Non-prescriptive
- Best practice.

ITIL is successful because it describes practices that enable organizations to deliver benefits, return on investment and sustained success.

1.3 Service management

A set of specialized organizational capabilities for providing value to customers in the form of services

IT service: A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement (SLA). Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services.

The outcomes that customers want to achieve are the reason why they purchase or use a service. The value of the service to the customer is directly dependent on how well a service facilitates these outcomes.

Services can be classified as:

- Core services
- Enabling services
- Enhancing services

Service management enables service providers to:

- Understand the services they are providing
- Ensure that the services really do facilitate the outcomes their customers want to achieve
- Understand the value of the services to their customers
- Understand and manage all of the costs and risks associated with those services.

Service management is concerned with more than just delivering services. Each service, process or infrastructure component has a lifecycle, and service management considers the entire lifecycle from strategy through design and transition to operation and continual improvement.

IT service management (ITSM): The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.

1.4 Processes and functions

Processes have the following characteristics:

- Measurability
- Specific results
- Customers
- Responsiveness to specific triggers

An organization needs to clearly define the roles and responsibilities required to undertake the processes and activities involved in each lifecycle stage. These roles are assigned to individuals within an organizational structure of teams, groups or functions

1.5 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. One person or team may have multiple roles. Roles fall into two main categories

- generic roles
- specific roles

1.5.1 Process owner

The process owner role is accountable for ensuring that a process is fit for purpose, i.e. that it is capable of meeting its objectives; that it is performed according to the agreed and documented standard; and that it meets the aims of the process definition. This role may be assigned to the same person carrying out the process manager role. Key accountabilities include:

- Sponsoring, designing and change managing the process and its metrics
- Defining the process strategy, with periodic reviews to keep current, and assisting with process design
- Defining appropriate policies and standards for the process, with periodic auditing to ensure compliance
- Communicating process information or changes as appropriate to ensure awareness
- Providing process resources to support activities required throughout the service lifecycle
- Ensuring that process technicians understand their role and have the required knowledge to deliver the process
- Addressing issues with the running of the process

- Identifying enhancement and improvement opportunities and making improvements to the process.

1.5.2 Process manager

The process manager role is accountable for operational management of a process. There may, for example, be several process managers for one process in different locations. This role may be assigned to the same person carrying out the process owner role. Key accountabilities include:

- Working with the process owner to plan and coordinate all process activities
- Ensuring that all activities are carried out as required throughout the service lifecycle
- Appointing people to the required roles and managing assigned resources
- Working with service owners and other process managers to ensure the smooth running of services
- Monitoring and reporting on process performance
- Identifying opportunities for and making improvements to the process.

1.5.3 Process practitioner

A process practitioner is responsible for carrying out one or more process activities. This role may be assigned to the same person carrying the process manager role, if appropriate. Responsibilities typically include:

- Carrying out one or more activities of a process
- Understanding how his or her role contributes to the overall delivery of service and creation of value for the business
- Working with other stakeholders, such as line managers, co-workers, users and customers, to ensure that their contributions are effective
- Ensuring that the inputs, outputs and interfaces for his or her activities are correct
- Creating or updating records to show that activities have been carried out correctly.

1.5.4 Service owner

The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and is accountable to the IT director or service management director for the delivery of a specific IT 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. Service ownership is critical to service management and one person may fulfil the service owner role for more than one service. Key responsibilities include:

- Ensuring that the ongoing service delivery and support meet agreed customer requirements via effective service monitoring and performance
- Working with business relationship management to ensure that the service provider can meet customer requirements
- Ensuring consistent and appropriate communication with customers for service-related enquiries and issues

- Representing the service across the organization; for example, by attending change advisory board meetings
- Serving as the point of escalation (notification) for major incidents relating to the service
- Participating in internal and external service review meetings
- Participating in negotiating SLAs and operational level agreements (OLAs) relating to the service
- Identifying opportunities for, and making, improvements to the service.

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.

1.5.5 The RACI model

the RACI model or 'authority matrix' can be used to define the roles and responsibilities in relation to processes and activities.

- Responsible
- Accountable
- Consulted
- Informed

Only one person should be accountable for any process or individual activity, although several people may be responsible for executing parts of the activity.

1.6 Release, control and validation supporting the service lifecycle

1.6.1 Purpose and objectives

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. 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.

1.6.2 Scope

The scope of service transition includes planning, building, testing, evaluation and deployment of all changes to services and service assets. Consideration is given to:

- Managing the complexity associated with changes to services and processes
- Allowing for innovation while minimizing the unintended consequences of change
- Introducing new services

- Changing existing services (e.g. expanding, reducing or changing suppliers)
- Retiring services, applications or other configuration items (CIs).

The scope of service transition includes guidance on transferring services:

- Out to a new supplier (outsourcing or offshoring), in from a supplier (insourcing), or out to a shared service provision
- From one supplier to another
- To multiple suppliers (smart sourcing), partnering or joint ventures
- As part of mergers and acquisitions.

The scope also includes the transition of changes in a service provider's service management capabilities that will impact on the ways of working, the organization, people, projects and third parties involved in service management.

1.6.3 Value to business of service transition activities

- Enable projects to plan the service transition stage more accurately, allowing service transition assets to be shared and re-used
- Result in higher volumes of successful change
- 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.

1.6.4 Transition strategy

The service transition strategy defines the overall approach to organizing service transition and allocating resources, including:

- Purpose and objectives of service transition
- Context (e.g. service customer, contract agreement portfolio)
- Scope (inclusions and exclusions)
- Applicable standards, agreements, legal, regulatory and contractual requirements
- Organizations and stakeholders involved in transition
- Framework for service transition, including criteria, approach and deliverables
- Identification of requirements and content of the new or changed service
- Schedule of milestones
- Financial requirements (budgets and funding).

1.6.5 Service transition lifecycle stages

The service design package (SDP) defines the lifecycle stages for service transition. The move from one stage to the next is subject to formal checks. Typical stages in the life of a transition include:

- Acquire and test new CIs and components

- Build and test
- Service release test
- Service operational readiness test
- Deployment
- Early life support
- Review and close service transition.

1.6.6 Preparing for service transition

- Reviewing and acceptance of inputs from the other service lifecycle stages
- Reviewing and checking the input deliverables, such as the change proposal, SDP, service acceptance criteria and evaluation report
- Identifying, raising and scheduling requests for change (RFCs)
- Checking that the configuration baselines are recorded in the configuration management system (CMS) before the start of service transition
- Checking transition readiness.

Any variance in the proposed service scope, service strategy requirements and service design baseline must be requested and managed through change management.

1.6.7 Planning and coordinating service transition

1.6.7.1 Planning an individual service transition

A service transition plan describes the tasks and activities required to release and deploy a release into the test environments and into production, including:

- Work environment and infrastructure for the service transition
- Schedule of milestones, handover and delivery dates
- Activities and tasks to be performed
- Staffing, resource requirements, budgets and timescales at each stage
- Issues and risks to be managed
- Lead times and contingency.

1.6.7.2 Integrated planning

Good planning and management are essential for successful deployment of a release into production across distributed environments and locations

1.6.7.3 Adopting programme and project management best practice

It is best practice to manage several releases and deployments as a programme, with each significant deployment run as a project.

1.6.7.4 Reviewing the plans

Review all service transition and release and deployment plans. Lead times should include an element of contingency and be based on experience rather than just the supplier's assertion

1.6.8 Provide service transition support

1.6.8.1 Advice

Service transition provides support for all stakeholders to enable them to understand and follow the service transition framework of processes, supporting systems and tools

1.6.8.2 Administration

Transition planning and support provides administration for:

- Managing service transition changes and work orders
- Managing issues, risks, deviations and waivers
- Managing support for tools and service transition processes
- Monitoring the service transition performance to provide input into continual service improvement.

Changes that affect the agreed baseline CIs are controlled through change management.

1.6.8.3 Communication

Managing communication throughout a service transition is critical to success. A communication plan should include:

- Objectives of the communication
- Defined stakeholders, including users, customers, IT staff, suppliers and customers of the business (if appropriate)
- Communication content for each type of stakeholder
- Communication frequency (daily, weekly etc.); this may vary for each stakeholder group at different stages of the transition
- Channel and format (newsletters, posters, emails, reports, presentations etc.)
- How the success of the communication will be measured.

1.6.8.4 Progress monitoring and reporting

Monitor service transition activities against the intentions set out in the transition model and plan. Measuring and monitoring the release and deployment establishes whether the transition is proceeding according to plan.

1.6.9 Processes within service transition

- Transition planning and support
- Change management
- Service asset and configuration management
- Release and deployment management
- Service validation and testing
- Change evaluation
- Knowledge management.

2 Change management

2.1 Purpose and objectives

Changes arise for a variety of reasons:

- Proactively
- Reactively

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. The objectives of change management are to:

- Respond to changing business requirements, while maximizing value and reducing incidents, disruption and rework
- Respond to requests for change (RFCs) from the business and IT that will align the services with the business needs
- Ensure 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 CIs are recorded in the configuration management system (CMS)
- Optimize overall business risk.

2.2 Scope

The scope of change management includes changes to baseline service assets and CIs across the whole service lifecycle.

Each organization should define which changes are outside the scope of its service change process. Typically these include:

- Changes with significantly wider impact than service changes, such as changes to business operations
- Changes at an operational level, such as repair to a printer.

2.3 Value to the business

- Protecting the business, and other services, while making required changes
- Implementing changes that meet customers' requirements while optimizing costs
- Contributing to governance, legal, contractual and regulatory requirements
- Reducing failed changes, service disruptions, defects and rework
- Improving service availability by improving the speed and success of corrective changes
- Reducing the time and effort needed to manage changes.

2.4 Policies, principles and basic concepts

Change management needs executive support to implement a culture that sets stakeholder expectations about changes and releases. This helps to manage any pressures to reduce timescales, cut budgets or compromise testing.

Policies that support change management include:

- Creating a culture of change management across the organization where there is zero tolerance for unauthorized change
- Aligning with business, project and stakeholder change management
- Prioritization of change and management of change windows
- Establishing accountability, responsibilities and segregation of duties
- Preventing unauthorized change
- Performance and risk evaluation of all changes.

Change management should be planned with release and deployment management and service asset and configuration management. The design includes:

- Requirements (legal, regulatory, standards, organizational practices)
- Approach to eliminating unauthorized change
- Techniques for identification and classification of changes
- Roles and responsibilities (for authorization, testing, CAB membership, other stakeholders etc.)
- Communication (changes, schedules, release plans)
- Procedures for all change activities
- Interfaces with other service management processes (especially configuration, release and deployment, incident and problem management).

2.4.1 Types of change request

A change request is a formal communication seeking an alteration to one or more CIs. This may be in the form of a request for change (RFC), but it could also be a service desk call, a formal request for change within a project, or some other similar formal communication. Change management applies across the entire service lifecycle, not just during the operational stage.

There are three different types of service change:

- Standard change
- Emergency change
- Normal change

A change process model can help to ensure that a particular type of change is handled in a consistent way.

Change proposals are submitted to change management before chartering new or changed services to ensure that potential conflicts for resources or other issues are identified.

Authorization of the change proposal does not authorize implementation of the change but allows the service to be chartered so that service design activity can start.

No change should be authorized unless you have explicitly defined what to do if it is not successful.

If changes are not reversible an alternative approach to remediation is required, such as revisiting the change itself

2.5 Process activities, methods and techniques

2.5.1 Create and record the request for change

The change initiator fills in an RFC, which ensures that all the required information is supplied. The RFC may be recorded on paper or electronically

If this is a major change with significant implications then a change proposal is required. A change proposal is used to communicate a high-level description of the change. This change proposal is normally created by the service portfolio management process and is passed to change management for authorization.

2.5.2 Review request for change

Change management carries out an initial review and rejects changes that are incomplete, totally impractical, or that duplicate other RFCs (accepted, rejected or still under consideration).

2.5.3 Assess and evaluate change

An assessment of the potential impact of the change is carried out. Generic questions such as the 'seven Rs' are a good starting point:

- Who raised the change?
- What is the reason for the change?
- What is the return required from the change?
- What are the risks involved in the change?
- What resources are required to deliver the change?
- Who is responsible for the build, test and implementation of the change?
- What is the relationship between this change and other changes?

Considerations for an impact and resource assessment include:

- Impact on the customer's business operation
- Effect on the IT infrastructure and on non-IT infrastructure, such as security and transport
- Effect on the service and on other services
- Impact of not implementing the change
- IT, business and other resources needed to implement the change, and for ongoing support of the changed service
- The current change schedule and projected service outage
- Impact on plans for continuity, capacity, security, testing and operation.

2.5.4 Authorize change

Levels of authority for the various types of change are as follows:

- For very significant changes the CAB may pass the request to a higher-level authority such as a global CAB, or the board of directors.
- For minor changes the change authority may be an operations supervisor or the change manager, or another suitably placed person. This authority is defined as part of the overall change management process.
- For emergency changes the change authority may be the emergency change advisory board (ECAB), if it is not practical to convene a meeting of the full CAB in the time available.

2.5.5 Coordinate change implementation

Authorized change requests are formally passed to an appropriate technical group to build the change. This activity is carried out as part of the release and deployment management process.

Change management is responsible for coordinating activities to manage the change schedule. This includes ensuring all testing is complete, and that implementation and remediation plans are in place.

2.5.6 Review and close change record

The results of every change are reported for evaluation and presented as a completed change for stakeholder agreement. This evaluation is carried out as part of the evaluation process.

A change review or post-implementation review confirms the change has met its objectives. The review includes incidents caused by the change, and achievement of service targets by any third parties involved. Change management (or the CAB) decides what action to take if changes have not met their objectives.

2.6 Managing organization and stakeholder change

The five key elements of change are necessity, vision, plan, resources and competence. It is important that management commits to these five requirements in any change. The management board or executive must provide a clear strategic vision. Factors that drive successful organizational change initiatives include:

- Leadership for the change
- Organization adoption
- Governance
- Organization capabilities
- Business and service performance measures
- A strong communication process with regular opportunity for staff feedback.

Service transition must be actively involved in changing the mindsets of people across the lifecycle to ensure they are ready to play their role in service transition. These people include:

- Service transition staff
- Customers

- Users
- Service operation functions
- Suppliers
- Key stakeholders.

Service transition focuses on simple messages to ensure that there is consistency in the implementation of the changes. For example, service transition would be interested in helping people to:

- Understand the need for knowledge and effective knowledge transfer
- Understand the importance of making decisions at the right speed and within the appropriate timeframe
- Understand the need to complete and review configuration baselines in a timely manner
- Apply more effective risk assessment and management methods for service transition
- Follow the deadlines for submitting changes and releases.

2.7 Triggers, inputs, outputs and interfaces

Strategic changes may arise from:

- Changes to legislation, regulations, policy or standards
- Organizational changes or changes to patterns of business activity
- Addition of new services or other updates to the service portfolio, customer portfolio or contract portfolio
- Sourcing changes and technology innovations.

Changes to planned services (in the service pipeline) and to existing services (in the service catalogue) may result in updates to:

- Service catalogue, service packages, definitions or characteristics
- Service level requirements, warranties or utilities
- Predicted capacity, quality, value or performance
- Release packages, acceptance criteria or communication plans
- Service assets (including infrastructure such as buildings)
- Processes or plans, such as capacity, IT service continuity management and test plans
- Procedures, measurement systems and documentation.

Inputs include:

- Policies, plans and strategies for change, release, deployment, evaluation etc.
- Change proposals and RFCs
- Change schedule and projected service outage
- Current assets, baselines, service packages, release packages etc.
- Test results, test reports and evaluation report.

Outputs include:

- Rejected and approved RFCs
- Updates to the service portfolio and service catalogue
- Changes to services and other CIs
- Revised change schedule and projected service outage
- Authorized change plans and updated change documentation, records and reports.

Interfaces within IT service management (ITSM) include:

- Service asset and configuration management (SACM)
- Problem management
- IT service continuity management
- Information security management
- Capacity management and demand management
- Service portfolio management.

Interfaces outside ITSM include:

- Business change processes
- Program and project management
- Organizational and stakeholder change management
- Sourcing and partnering.

2.8 Critical success factors and key performance indicators

- CSF Responding to RFCs from the business and IT that align the services with the business needs while maximizing value:
 - KPI Increase in the percentage of changes that meet the customer's agreed requirements; for example, quality, cost, time
 - KPI The benefits of change (expressed as 'value of improvements made' + 'negative impacts prevented or terminated') exceed the costs of change
- CSF Optimizing overall business risk:
 - KPI Reduction in the number of disruptions to services, defects and rework caused by inaccurate specification, poor or incomplete impact assessment
 - KPI Reduction in the percentage of changes that are categorized as emergency changes
- CSF Ensuring that all changes to CIs are well managed and recorded in the CMS:
 - KPI Reduction in the number and percentage of changes with incomplete change specifications
 - KPI Reduction in the number and percentage of changes with incomplete impact assessments.

2.9 Challenges and risks

Challenges include:

- Ensuring that every change is recorded and managed
- Being seen to facilitate change, rather than to introduce delays
- Implementing a true change management process that becomes involved early enough in the service lifecycle, includes assessment of benefits and costs, and helps to plan and manage changes
- Agreeing and documenting the many levels of change authority that are needed to manage change effectively and enabling effective communication between these change authorities.

Risks include:

- Lack of commitment to the change management process from the business, IT management or 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
- Introducing delays to change implementation without adding sufficient value
- Insufficient time or resources being allowed for proper assessment of changes, and pressure from projects or the business to expedite decisions
- Insufficient time being allowed for implementation of changes, and attempting to fit too many changes into a change window
- Lack of clarity on how change management interacts with other service management processes, project management or service design activities
- Excessively bureaucratic change management processes that introduce excessive delay to required changes.

2.10 Typical day-to-day activities performed by service operation

- Raising and submitting RFCs to address service operation issues
- Assessing changes and participating in CAB or ECAB meetings
- Implementing or backing out changes as directed by change management
- Helping to define and maintain change models
- Using the change management process for operational changes.

2.11 Roles and responsibilities

2.11.1 Change management process owner

- Carrying out the generic process owner role for the change management process
- Designing the 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.

2.11.2 Change management process manager

- Carrying out the generic process manager role for the change management process (see section 1.5 for more detail)
- Receiving, logging and assigning priority to all RFCs and rejecting incomplete or totally impractical RFCs
- Deciding whom to invite to CAB meetings, issuing invitations and agenda, and circulating RFCs in advance for review
- Convening CAB or ECAB meetings, considering advice from the CAB or ECAB, and authorizing acceptable changes
- Communicating with users and the business, including publishing the change schedule and projected service outage
- Coordinating the build, test and implementation of the change, and updating the change log with progress
- Reviewing all changes, identifying opportunities for improvement and producing management reports.

Depending on the size of the organization, the change management process manager may also be the process owner for the change management process.

2.11.3 Change initiator

- Identifying the requirement for a change
- Completing and submitting a change proposal if appropriate
- Completing and submitting an RFC
- 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.

Many different people in the organization may carry out this role; it is not usually carried out by people who work in change management. Each change has a single change initiator.

2.11.4 Change 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.

2.11.5 Change authority

- Reviewing specific categories of RFC
- Formally authorizing changes at agreed points in the change lifecycle
- Participating in the change review before changes are closed
- Attending CAB meetings to discuss and review changes when required.

There are normally different change authorities for each category of change.

3 Service asset and configuration management

3.1 Purpose and objectives

The purpose of the service asset and configuration management (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. This information includes details of how the assets have been configured and the relationships between them.

The objective of SACM is to define and control components of services and infrastructure, and to maintain accurate information on the planned, current and historical state of services and infrastructure.

3.2 Scope

The scope of SACM depends on the size of the implementing organization, but some scoping statements are valid for implementations of any scale or with any objectives:

- Asset management covers the lifecycle of service assets from acquisition to disposal. It provides a complete inventory of assets and who is responsible for their control
- Configuration management ensures that components of a service, system or product are identified, baselined and maintained. It provides a configuration model of services, assets and infrastructure by recording relationships between service assets and CIs
- SACM is accountable for the accuracy of the data within the configuration management system (CMS).

3.3 Value to the business

- Changes and releases to be assessed, planned and delivered successfully
- Assistance in speeding up incident resolutions
- Better adherence to standards and regulatory obligations
- The ability to identify the full cost model of delivering a service
- Easy access to information on all assets and CIs held within the CMS
- Proper stewardship of fixed assets that are under the control of the service provider.

3.4 Policies, principles and basic concepts

The first step is to develop and maintain the SACM policies that set the objectives, scope, principles and critical success factors (CSFs) for what is to be achieved by the process.

SACM needs change management to make it effective. The maintenance of the CMS is the responsibility of SACM, but change management enables the CMS's accuracy to be maintained.

Typical principles include:

- The need to meet corporate governance requirements such as Sarbanes-Oxley
- The need to deliver capability, resources and warranties defined by service level agreements (SLAs)

- The requirement for available, reliable and costeffective services
- The application of whole-life cost appraisal methods
- The requirement to maintain asset and configuration information for stakeholders
- The level of control and requirements for traceability and auditability
- The provision of information for other business and service management processes.

3.4.1 The configuration model

SACM delivers a logical model of the services, assets and infrastructure by recording relationships between CIs. The real power of this model is that it is a single model, used by all parts of IT service management and beyond; it potentially includes human resources, finance, suppliers and customers. This enables other processes to access valuable information so they can:

- Assess the impact and cause of incidents and problems
- Assess the impact of proposed changes
- Plan and design new or changed services, technology refreshes and software upgrades
- Plan release and deployment packages, and migrate service assets to different locations and service centres.

3.4.2 Configuration items

Common categories for CIs include:

- Service lifecycle CIs
- Service CIs
- Organization CIs
- Internal CIs
- External CIs
- Interface CIs

3.4.3 The configuration management system

To manage large and complex IT services and infrastructures, SACM requires the use of a CMS, with a layered architecture. This includes layers for data, information, knowledge processing and presentation.

The CMS holds all information for CIs within the designated scope. It maintains the relationships between CIs and related incidents, problems, known errors, change and release documentation. It may also include data about employees, suppliers, locations, customers and users.

The CMS includes one or more configuration management databases (CMDBs) and definitive media libraries (DMLs) as well as other data. It provides access to data in other inventories wherever possible, rather than duplicating data.

The CMS integrates and manages a number of other SACM concepts, including:

- Secure libraries

- DMLs
- Secure stores
- Definitive spares
- Baselines
- Snapshots

3.5 Process activities, methods and techniques

3.5.1 Management and planning

The management team decides on the scope and what level of detail is needed, and documents this in a configuration management plan. A typical plan includes:

- Scope
- Requirements
- Applicable policies and standards
- Organization for SACM
- System tools
- Application of processes and procedures
- Reference implementation plan
- Relationship management and control of suppliers and subcontractors.

There may also be separate configuration management plans for individual projects, services or groups of services.

3.5.2 Configuration identification

- Define how CIs are to be selected, grouped, classified and defined
- Define the approach to identification, naming and labelling
- Define the roles and responsibilities of the CI owner

Configuration identification steps are:

- Select the CIs based on documented criteria, and assign a unique name to each
- Specify the relevant attributes and relationships:
 - Attributes describe the characteristics of a CI that are valuable to record and that support service management processes
 - Relationships describe how the CIs work together; for example, a parent–child relationship; connected to; part of; or installed on. Relationships may be one-to-one, one-to-many or many-to-one; for example, many applications may be installed on one server
- Specify when each CI is placed under configuration management; for example, when it is released and when it is acquired
- Identify the owner of each CI.

3.5.3 Configuration control

Configuration control ensures that there are control mechanisms over CIs, and maintains a record of changes to CIs, status, versions, location and ownership

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

Control should be passed from a project or supplier to the service provider at the scheduled time with accurate configuration information, documentation and records.

3.5.4 Status accounting and reporting

Each asset or CI has one or more discrete states through which it can progress. The list of valid status codes depends on the CI type.

3.5.5 Verification and audit

- Ensure there is conformity between the documented baselines and the actual business environment
- Verify the physical existence of CIs and check that the records in the CMS match the physical infrastructure
- Verify that every physical component has a record in the CMS-Check that required release and configuration documentation is in place before making a release.

Plans are needed to ensure regular configuration audits are carried out, to check that the CMDBs and related configuration information are consistent with the physical state.

3.6 Asset management

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

3.7 Triggers, inputs, outputs and interfaces

Updates to SACM information are triggered by changes, purchase orders, acquisitions and service requests.

Inputs include:

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

Outputs include:

- New and updated configuration records
- Updated asset information for use in updating the fixed asset register

- Information about attributes and relationships of CIs, for use by all other service management processes
- Configuration snapshots and baselines
- Status reports and other consolidated configuration information
- Audit reports.

As the single repository for configuration data, SACM supports and interfaces with every other process, function and activity. There are strong relationships with:

- Change management
- Financial management
- IT service continuity management
- Incidents, problems and errors

3.8 Information management

Backup copies of the CMS are taken regularly and stored securely, preferably off-site to enable access when IT service continuity management is invoked.

3.9 Critical success factors and key performance indicators

- CSF Accounting for, managing and protecting the integrity of CIs throughout the service lifecycle:
 - KPI Improved accuracy in budgets and charges for the assets utilized by each customer or business unit
 - KPI Increase in re-use and redistribution of under-utilized resources and assets
- CSF Supporting efficient and effective service management processes by providing accurate configuration information at the right time:
 - KPI Percentage improvement in maintenance scheduling over the life of an asset (not too much, not too late)
 - KPI Improved speed for incident management to identify faulty CIs and restore service
- CSF Establishing and maintaining an accurate and complete CMS:
 - KPI Reduction in business impact of outages and incidents caused by poor service asset and configuration management
 - KPI Increased quality and accuracy of configuration information.

3.10 Challenges and risks

Challenges include:

- Persuading technical support staff to adopt a policy of checking everything in and out – this can be perceived as a hindrance to a fast and responsive support service. If the positives of such a system are not conveyed adequately, staff may be inclined to try and circumvent it. Even then, resistance can still occur – placing this as an objective in annual appraisals is one way to help enforce the policy.

- Attracting and justifying funding for SACM, since it is typically unseen by the customer units empowered with funding control. In practice it is typically funded as an 'invisible' element of change management and other ITSM processes that are more visible to the business.
- An attitude of 'just collecting data because it is possible to do it'; this leads SACM into a data overload, which is impossible, or at least disproportionately expensive, to maintain.
- Lack of commitment and support from management who do not understand the key role SACM must play in supporting other processes.

Risks include:

- The temptation to consider SACM to be technically oriented rather than service and business focused, since technical competence is essential to its successful delivery
- Degradation of the accuracy of configuration information over time, which can cause errors and be difficult and costly to correct
- Setting the scope too wide, causing excessive cost and effort for insufficient benefit
- Setting the scope too narrow, so that the process has too little benefit
- The CMS becoming out of date due to the movement of hardware assets by non-authorized staff. To prevent this, undertake regular physical audits to highlight discrepancies, investigate them, and inform managers of any inconsistencies.

3.11 Typical day-to-day activities performed by service operation

- Informing SACM of any discrepancies found between CIs and the CMS
- Making agreed amendments to correct discrepancies.

Responsibility for updating the CMS remains with SACM, but in some cases staff working within service operation functions may be asked to update relationships, add new CIs or amend the status of CIs.

3.12 Roles and responsibilities

During the first stages of a project, the programme or project office may be responsible for configuration management. At defined release points this responsibility is passed to staff working within service transition, and SACM takes over the responsibility for CI documentation.

3.12.1 SACM process owner

- Carrying out the generic process owner role for the SACM process (see section 1.5 for more detail)
- Agreeing the scope for SACM and policies
- Working with other process owners to ensure integration.

3.12.2 SACM process manager

- Carrying out the generic process manager role for the SACM process (see section 1.5 for more detail)

- Responsible for planning, implementing, monitoring and improving configuration management as a process.

3.12.3 Configuration analyst

- Working with the SACM process manager to plan aspects of configuration management, such as which CIs should be managed and to what level
- Training other configuration management staff and performing configuration audits.

3.12.4 Configuration librarian

Responsibilities include being the custodian and guardian of master copies of software, assets and documentation.

4 Service validation and testing

4.1 Purpose and objectives

The purpose of the service validation and testing process is to ensure that a new or changed IT service matches its design specification and meets the needs of the business. The objectives of service validation and testing are to:

- Assure people that the new or changed services will provide the expected outcomes and value within the cost, capacity and constraints identified
- Validate a service to make sure that it is 'fit for purpose'
- Ensure that a service is 'fit for use'
- Confirm that requirements for new or changed services are defined correctly
- Find any errors and variances and remedy them early in the service lifecycle.

4.2 Scope

Service validation and testing can be applied throughout the service lifecycle to ensure the quality of:

- Any aspect of any new or changed service or service offering, including:
 - Services developed in-house or externally
 - Hardware, software or knowledge-based services
- The service provider's capability, resources and capacity to deliver a service or service release.

Validation and testing of an end-to-end service requires:

- Interfaces with suppliers, customers and partners
- Defined boundaries of the service to be tested, including process and organizational interfaces.

As well as covering the functionality of the components, testing examines their behaviour in conjunction with their intended use in the target business unit, service unit, deployment group or environment.

Testing supports the release and deployment process, ensuring the correct levels of testing have been undertaken, including the validation of the proposed service models as being 'fit for use' and 'fit for purpose' before authorization is given to enter service operation.

Information obtained during service validation and testing can be used to assess the performance of the live system as part of the change evaluation process.

4.3 Value to the business

Key values that the business and the customer gain from service testing and validation are confidence that a new or changed service will deliver the required value and outcomes, and an understanding of the risks.

4.4 Policies, principles and basic concepts

Service validation and testing is driven by policies for:

- Service quality
- Risk
- Service transition (not covered in this publication)
- Release
- Change management.

4.4.1 Service quality policy

- Level of excellence
- Value for money
- Conformance to specification
- Meeting or exceeding expectations.

4.4.2 Risk policy

This can vary considerably depending on factors such as the business's appetite for risk, regulations and safety criticality.

4.4.3 Release policy

The level and type of testing are influenced by type and frequency of releases.

4.4.4 Change management policy

The use of change windows can influence the testing that needs to be considered

4.4.5 Test models

Test models help to ensure consistency and repeatability, improving effectiveness and efficiency. Contents of a test model include a test plan ('What is to be tested?') and test scripts (including test conditions and expected results). To ensure the test model is repeatable it needs to be well structured.

Test models use service design and release plans to determine specific requirements. Separate test models can be created for the different types/stages of testing.

4.4.6 Validation and testing perspectives

The focus of validation and testing is to confirm that the service delivered fulfils all the agreed criteria, including the ability to deliver, deploy, use, manage and operate the service during its lifetime. The service design package (SDP) documents entry and exit criteria for each level and area of testing.

Perspectives to be considered include design of the service, technology, processes and measurements as well as documentation, skills and knowledge.

4.4.7 Business user and customer perspective

Acceptance testing by the business is included in the SDP. The importance of this to the business is that it enables:

- Measurement of acceptability of the service, including interfaces with the service provider
- Understanding of the resources needed to undertake the acceptance testing.

The importance of this to the service provider is that it:

- Maintains business involvement through the lifecycle, avoiding last-minute surprises
- Manages business perceptions of reliability and usability before the service goes live
- Provides acceptance test facilities to meet business requirements
- Improves understanding of the links between acceptance testing and other business activities.

The period of acceptance testing allows the customer and users to become familiar with the new service well before live operation, reducing any initial resistance to change.

4.4.8 User testing – application, system and service

The areas that are covered include:

- Required functionality
- Changed business processes
- Service management activities, such as contact with the service desk.

The scope and coverage of the tests are defined in the user test or user acceptance test plan.

4.4.9 Operations and service improvement perspective

Service acceptance checks that the following have been considered before deployment:

- Technology and facilities
- Support staff with requisite skills and knowledge
- Supporting processes correctly resourced and in place (for example, the service desk)
- Business and IT continuity
- Access to documentation and the service knowledge management system (SKMS).

4.4.10 Levels of testing and testing models

Each service asset and component needs to be tested to ensure it meets the business, user and operational requirements before it is used in the live operational environment.

A re-usable test model is developed for each service model and associated deliverables, enabling regression-testing of specific releases for initial and subsequent deployments.

4.5 Process activities, methods and techniques

The activities do not have to be undertaken sequentially; several can be done in parallel.

4.5.1 Validation and test management

- Resource planning, activity prioritization and scheduling
- Management of incidents, problems, errors, non-conformances, risks and issues
- Monitoring and reporting, including collection, analysis and reporting on metrics
- Introduction of changes to reduce potential errors
- Capturing configuration baselines.

4.5.2 Plan and design tests

- Resourcing, including business and customer resources
- Hardware/networks
- Supporting services
- Schedule/milestones, including time allocation for review and acceptance of reports and other interim deliverables, and details for delivery and acceptance of products
- Budgets and financial requirements.

4.5.3 Verify test plan and test designs

- Appropriate test coverage for the level of risk
- Coverage of integration and interface aspects
- Examination of the accuracy and completeness of test scripts.

4.5.4 Prepare test environment

Use build and test environment staff to create a suitable test environment with the assistance of the release and deployment management process. Take a configuration baseline once the initial test environment has been created.

4.5.5 Perform tests

Tests can be automated or executed manually. Record the tests to measure those that have run successfully and to raise incidents for any test failures, enabling the creation of resolutions or known errors.

Any updates will be retested, preferably by the same tester. The deliverables from the activity are:

- Actual results with reference to the tests undertaken
- Outstanding problems, issues, risks etc. awaiting resolution
- Resolved problems, issues, risks etc. and associated changes
- Testing sign-off.

4.5.6 Evaluate exit criteria and report

This activity matches the actual result of the testing phase against the expected result and identifies any differences that would:

- Increase the risk to the business or service provider
- Change the projected value.

4.5.7 Test clean-up and closure

Ensure that test environments are cleaned up or initialized. Review the testing approach and identify any improvements that could be made.

4.6 Triggers, inputs, outputs and interfaces

Testing activities are scheduled in test, release or quality assurance plans.

Inputs include:

- SDP
- RFCs

A key output is a report that is passed to change evaluation providing details of:

- The configuration baseline of the test environment
- Testing that was carried out and the results
- Risks identified when comparing expected and actual results.

Additional outputs are:

- Data, information and knowledge
- Test incident, problem and error records
- Ideas for any improvements to the testing process and service design outputs.

Successful testing requires interfaces with:

- Service design, to ensure designs are testable and support testing activities
- Service transition, to support all release and deployment steps
- Continual service improvement, to provide feedback about failures and areas where improvement would be beneficial
- Service operation, for handover of changed maintenance tests.

4.7 Information management

Service validation and testing benefits from the ability to re-use tests. To facilitate re-use, the test management group is responsible for creating, cataloguing and maintaining test-ware. The use of CAST (computer-aided software testing) tools can also be beneficial.

Information is required on the following, to ensure realistic testing can take place:

- Test data
- Test environments
- Active maintenance of test data

4.8 Critical success factors and key performance indicators

- CSF Understanding the different stakeholder perspectives that underpin effective risk management for the change impact assessment and test activities:
 - KPI Roles and responsibilities for impact assessment and test activities have been agreed and documented
 - KPI Increase in the number of new or changed services for which all roles and responsibilities for customers, users and service provider personnel have been agreed and documented
- CSF Building a thorough understanding of risks that have impacted or may impact successful service transition of services and releases:
 - KPI Reduction in the impact of incidents and errors for newly transitioned services
 - KPI Increased number of risks identified in service design or early in service transition compared to those detected during or after testing.

4.9 Challenges and risks

The most frequent challenges to effective testing are caused by a lack of respect for and understanding of the role of testing. Traditionally, testing has been starved of funding, resulting in:

- Inability to maintain a test environment and test data that match the live environment
- Insufficient staff, skills and testing tools to deliver adequate testing coverage
- Projects overrunning and allocated testing timeframes being squeezed to restore project go-live dates, but at the cost of quality
- Development of standard performance measures and measurement methods across projects and suppliers
- Projects and suppliers estimating delivery dates inaccurately and causing delays in scheduling service transition activities.

Risks include:

- Unclear expectations and objectives
- Lack of understanding of the risks resulting in testing that does not target the critical elements that need to be well controlled
- Resource shortages (e.g. users, support staff), that introduce delays and have an impact on other service transitions.

4.10 Roles and responsibilities

4.10.1 Service validation and testing process owner

- Carrying out the generic process owner role for the service validation and testing process
- Defining the overall test strategy for the organization
- Working with other process owners to ensure that there is an integrated approach to the design and implementation of change management, change evaluation, release and deployment management, and service validation and testing.

4.10.2 Service validation and testing process manager

- Carrying out the generic process manager role for the service validation and testing process (see section 1.5 for more detail)
- Helping to design and plan testing conditions, test scripts and test data sets during the service design stage of the service lifecycle, to ensure appropriate and adequate coverage and control
- Allocating and overseeing test resources, ensuring that test policies are adhered to
- Verifying tests conducted by release and deployment management or other teams
- Managing test environment requirements
- Planning and managing support for service testing and validation tools and processes
- Providing management reporting on test progress, test outcomes, success rates, issues and risks.

It is important that this role is assigned to a different person from whoever is responsible for release and deployment management, to avoid conflicts of interest.

4.10.3 Service validation and testing practitioner

- Conducting tests as defined in the test plans and designs, and documented in the SDP
- Recording, analyzing, diagnosing, reporting and managing test events, incidents, problems and retest dependent on agreed criteria
- Administering test assets and components.

5 Release and deployment management

5.1 Purpose and objectives

The purpose of the release and deployment management process is to plan, schedule and control the build, test and deployment of releases, and to deliver the new functionality required by the business while protecting the integrity of existing services. The objectives of release and deployment management include:

- Comprehensive plans that support customer and business change projects
- Releases that can be built, installed, tested and deployed efficiently and on time
- New or changed services that can meet agreed requirements
- Minimal unpredicted impact on services and on the IT organization.

5.2 Scope

The scope of release and deployment management includes the processes, systems and functions needed to package, build, test and deploy releases in order to establish the service specified in the service design package (SDP).

5.3 Value to the business

- Delivering change faster, with optimized cost and risk
- Assuring that users are able to use new or changed services to support business goals
- Improving consistency and auditability of service transitions.

5.4 Policies, principles and basic concepts

Release and deployment management policies help the organization achieve the correct balance between cost, service stability and agility. Release and deployment management policies help release and deployment management personnel to make decisions that support the overall objectives of the business.

5.4.1 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 according to the organization's release policy. The unit may vary, depending on the type(s) or item(s) of service asset or service component such as software and hardware.

A 'release package' is a set of CIs that will be built, tested and deployed together as a single release. Each release will take the documented release units into account when designing the contents of the release package. The decision about what is an appropriate release unit is based on:

- Time and resources needed to build, test, distribute and implement
- Complexity of interfaces with other components
- Availability of resources in the test environment, and frequency and ease of change.

5.4.2 Deployment options

The components to be released, and the approach to be taken, are defined in the SDP. Common options include:

- 'Big bang' vs phased
- Push vs pull
- Automated vs manual

Release and deployment models help to achieve consistency and repeatability. They include:

- How to build the release package and the target environments
- Exit and entry criteria for each stage, including handover activities
- Roles and responsibilities, template schedules and supporting systems and tools.

Each release and deployment model includes all activities needed to plan, package, build, test, deploy and implement the release.

5.5 Process activities, methods and techniques

5.5.1 Planning

5.5.1.1 Release and deployment plans

Release and deployment plans should be based on overall service transition plans, use a release model, and be authorized by change management. They define:

- Scope and content of the release
- Risk assessment and risk profile for the release
- Stakeholders affected by the release, and approvers for the change request(s)
- Team responsible for release, resources needed, and approach to be taken.

5.5.1.2 Pass/fail criteria

Criteria must be defined for each authorization point, and must be published to stakeholders to set expectations.

5.5.1.3 Build and test

- Developing build plans from the SDP and design specifications
- Establishing logistics, lead times and build times to create environments
- Scheduling activities and testing the procedures for build and test
- Assigning resources, roles and responsibilities
- Defining and agreeing entry and exit criteria for build and test.

5.5.1.4 Planning pilots

Pilots test the service with some users before rolling it out to the whole user base. The scope of the pilot must be planned to provide enough testing with acceptable time and resources, and must include all stakeholders. Multiple pilots may be needed to support diverse organizations, or a

range of different trialling options. A pilot must collect feedback from users, customers, suppliers, and support staff. It also includes analysis of service desk calls, capacity, availability and other data on use and effectiveness.

Always roll back a pilot before the full deployment of the new service to ensure that a consistent release is deployed.

5.5.1.5 Planning release packaging and build

This includes developing mechanisms, plans and procedures for:

- Verifying entry/exit criteria
- Managing stakeholder change and communication, training people, transferring knowledge, and developing service management capability
- Ensuring that agreements and contracts are in place
- Agreeing schedules and developing procedures to build and deploy the release and manage licences

-Converting users and systems (including any required data migrations).

5.5.1.6 Deployment planning

Planners should be able to answer the following questions:

- What needs to be deployed? (The components and the business drivers for these)
- Who are the users? (Any special language or training needs?)
- Where are the users? (Are any users remote or mobile?)
- Who else needs to be prepared in advance? (Service desk, support staff)
- When does deployment need to be completed?
- What is the current service provider capability? (Systems, infrastructure, capacity etc.)

5.5.1.7 Logistics and delivery planning

This stage includes planning for when and how each release unit or service component will be delivered. It requires planning for:

- Lead times and how delays will be managed
- Checking components on delivery and secure storage
- Managing customs or other internationalization issues
- Decommissioning redundant hardware, licenses, contracts etc.
- Resources needed for any parallel running.

5.5.1.8 Financial/commercial planning

Before the deployment starts it may be necessary to check:

- Working capital – are sufficient funds available?
- Contracts, licenses, and intellectual property, including third-party software and rights to documentation

- Funding for supporting services.

5.5.2 Preparation for build, test and deployment

Before authorizing the build and test stage:

- Carry out an independent evaluation to ensure the service will deliver the required outcomes (see Chapter 7)
- Assign people and other resources
- Carry out training for release, deployment, build and test teams.

5.5.3 Build and test

Configuration baselines must be recorded in the CMS before and after build, installation or deployment. Release packages must be placed in the definitive media library (DML) and must always be taken from the DML. Procedures and documents are needed to manage the build and test. These include:

- Contracts, agreements, purchase requests, fulfilment, goods in etc.
- Health and safety guidelines, and security policies and procedures
- Management of licensing and intellectual property rights
- Acceptance and authorization
- Documentation for handover to service operation.

Verification of components includes:

- Establishing that they are genuine and have been properly acquired
- Checking that standard naming and labelling conventions have been applied
- Checking items against descriptions and documentation
- Checking that appropriate quality reviews have taken place
- Checking software for malicious additions such as viruses
- Ensuring that all changes have been approved by change management
- Ensuring appropriate use of the DML and CMS
- Managing the return of components that are not satisfactory.

The key activities to build a release package are:

- Assemble and integrate components in a controlled, reproducible way
- Create documentation for build and release
- Install and verify the release package and take a baseline
- Inform relevant parties that the release package is available for installation.

5.5.4 Service testing and pilots

Testing is based on a test strategy and test model. There are many different types of test, including:

- Service release test
- Service operations readiness test

- Deployment readiness test
- Service management test
- Service operations test
- Service level test
- User test
- Service provider interface test
- Deployment verification test
- Service rehearsal
- Pilot

5.5.5 Plan and prepare for deployment, and perform transfer, deployment and retirement

These stages include preparing for organizational change, assigning deployment activities to specific people, and actually carrying out the deployment

5.5.6 Verify deployment

- Does the new configuration baseline match the planned configuration?
- Are documentation updates correct?
- Are required communication and learning materials ready for distribution?
- Have roles been assigned? Are people prepared to operate and use the service? Do they have the information they need?
- Are measurement and reporting in place?

5.5.7 Early life support

During this stage, checks are carried out to ensure that all agreed service levels are being met. Performance data is collected and compared with targets. Service reports are created and issues are addressed. Early life support does not end until the agreed exit criteria have been met. These typically include:

- Users can use the service effectively and efficiently for business activities
- Service and process owners can manage and operate the service as agreed
- Progress is being made towards delivering the expected benefits
- Service level agreements (SLAs) are signed off and service levels are being consistently achieved
- Training, knowledge transfer, documentation and deliverables are signed off.

5.5.8 Review and close deployment, review and close service transition

The final stages are formal reviews to ensure that:

- All outstanding issues have been documented and addressed
- Opportunities for improvement have been captured.

5.6 Triggers, inputs, outputs and interfaces

Inputs include:

- One or more authorized RFCs
- The SDP, including service model and service acceptance criteria
- Service management plans and standards
- Release policy and release design from service design
- Release and deployment models, and template plans
- Entry and exit criteria for each stage of release and deployment.

Outputs include:

- New, changed or retired services
- Release and deployment plan
- Updated service catalogue and new or changed documentation
- Updates to service level packages, service models, SLAs, operational level agreements and contracts
- New, tested service capability, including organizational changes, applications, data, infrastructure, environment etc.
- Updated configuration management database (CMDB) with full audit trail of new or changed CIs
- Updated service management plans (e.g. capacity plan, continuity plan)
- Service transition report.

Interfaces include:

- Design coordination
- Transition planning and support
- Change management
- Service asset and configuration management
- Service validation and testing.

5.7 Information management

- New or changed CIs, including ownership, status, attributes and relationships
- New or changed locations or users
- Plans and records for installation, build, logistics, delivery, validation and testing, deployment, and training
- Known errors.

5.8 Critical success factors and key performance indicators

- CSF Ensuring integrity of a release package and its constituent components throughout the transition activities:
 - KPI Reduced number of CMS and DML audit failures related to releases
 - KPI Reduced number of deployments from sources other than the DML
- CSF Ensuring that the new or changed service is capable of delivering the agreed utility and warranty:

- KPI Reduced variance from service performance required by customers
- KPI Number of incidents against the service (low and reducing).

5.9 Challenges and risks

Challenges include:

- Developing standard measures across many projects and suppliers
- Managing schedule delays caused by projects and suppliers
- Understanding diverse stakeholder perspectives
- Understanding risks and building a risk management culture.

Risks include:

- Poorly defined scope and understanding of dependencies
- Staff who are not dedicated and have other responsibilities
- Inadequate management, policies or leadership
- Insufficient finance or delays in provision of money
- Insufficient control of changes, or poor implementation or back-out plans
- Technology limitations or issues.

5.10 Typical day-to-day activities performed by service operation

There are some aspects that service operation staff are involved with on a day-to-day basis. These include:

- Actual implementation actions regarding the deployment of new releases, under the direction of release and deployment management, where they relate to service operation components or services
- Participation in the planning stages of major new releases to advise on service operation issues
- The physical handling of CIs from and to the DML as required to fulfil their operational roles – while adhering to relevant release and deployment management procedures, such as ensuring that all items are properly booked out and back in
- Participation in activities to back out unsuccessful releases when these occur.

5.11 Roles and responsibilities

5.11.1 Release and deployment management 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 all aspects of service transition.

5.11.2 Release and deployment 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
- Coordinating interfaces between release and deployment management and other processes, especially change management, SACM, and service validation and testing.

5.11.3 Release packaging and build practitioner

- Establishing the knowledge, information, hardware, software and infrastructure needed for the release
- Building and testing the final release (prior to independent testing)
- Reporting outstanding known errors and providing input to final sign-off.

5.11.4 Deployment practitioner

Deployment staff deals with the final physical delivery of the service. They coordinate documentation and communications, and provide technical and application guidance and support.

5.11.5 Early life support practitioner

- Ensuring delivery and quality of user and support documentation
- Embedding all activities required for the service to be operated and maintained
- Providing initial performance reporting and risk assessment of performance
- Providing initial support for incidents and errors.

6 Request fulfilment

6.1 Purpose and objectives

Request fulfilment is the process responsible for managing all service requests from the users through their lifecycle.

The objectives of the request fulfilment process are to:

- Maintain user and customer satisfaction by handling all service requests in an efficient and professional manner
- Provide a channel for users to request and receive standard services for which there is a predefined authorization and qualification process
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services
- Assist with general information, complaints or comments.

6.2 Scope

Some organizations deal with service requests through their incident management process (and tools), with service requests being handled as a particular type of 'incident'

In an organization where large numbers of service requests have to be handled, and where the actions to be taken to fulfil those requests are very varied or specialized, it may be appropriate to handle service requests as a completely separate work stream.

6.3 Value to the business and service lifecycle

- Quick and effective access to standard services; this can improve business productivity and/or quality
- A less bureaucratic system for requesting and receiving access to existing or new services, reducing the cost of providing these services
- Where fulfilment is centralized, having more control over services can reduce costs as supplier negotiation is also centralized and support costs are lower.

6.4 Policies, principles and basic concepts

Examples of request fulfilment policies include:

- The request fulfilment activities follow a predefined process flow or model which includes all stages needed to fulfil the request, the individuals or support groups involved, target timescales and escalation paths
- The ownership of service requests resides with a centralized function; for example, the service desk, which monitors, escalates, dispatches and may also fulfil the request
- Service requests that impact CIs are usually fulfilled by implementing a standard change
- All requests are logged, controlled, coordinated, promoted and managed via a single system

- All requests are authorized before activities are undertaken to fulfil them.

6.4.1 Request models

Service request models (which typically include one or more standard changes in order to complete fulfilment activities) are defined, to ensure that frequently used service requests are handled consistently and meet agreed service levels.

6.4.2 Menu selection

Request fulfilment offers great opportunities for self-help. Users are offered a self-help menu from which they can select requests and provide details.

6.4.3 Request status tracking

Track requests throughout their lifecycle to support proper handling of requests and reporting on their status. Within the request fulfilment system, status codes may be linked to requests to indicate where they are in relation to the lifecycle

6.4.4 Financial approval

The cost of providing the service should first be established and submitted to the user for approval within their management chain. In some cases there may be a need for additional compliance approval, or wider business approval.

6.4.5 Coordination of fulfilment activities

Simple requests may be completed by the service desk, while others are forwarded to specialist groups and/or suppliers for fulfilment. The service desk monitors progress and keeps users informed throughout, regardless of the actual fulfilment source.

6.5 Process activities, methods and techniques

6.5.1 Request receipt, logging and validation

Fulfilment work on service requests should not begin until a formalized request has been received, typically from the service desk. All service requests must be fully logged

6.5.2 Request categorization and prioritization

Requests can be categorized in several ways: for example, by service, activity, type, function or CI type.

Prioritization is determined by taking into account both the urgency of the request (how quickly the business needs to have it fulfilled) and the level of impact it is causing

There may also be occasions when, because of particular business expediency, normal priority levels have to be overridden. Some organizations may also recognize 'VIPs' whose service requests are handled as a higher priority than normal.

6.5.3 Request authorization

No work to fulfil a request should be done until it is authorized. Requests can be authorized via the service desk or by having pre-authorized requests. Alternatively, authorization may need to come from other sources

Service requests that cannot be authorized are returned to the requester with the reason for the rejection. The request record is also updated to indicate the rejection status.

6.5.4 Request review

The request is reviewed to determine the appropriate group to fulfil it. As requests are reviewed, escalated and acted upon, the request record is updated to reflect the current request status.

6.5.5 Request model execution

A request model documents a standard process flow, setting out the roles and responsibilities for fulfilling each request type to ensure that the fulfilment activities are repeatable and consistent

Request models may be described as process steps and activities that are stored as reference documents in the service knowledge management system (SKMS). Alternatively they may be stored through specialized configurations within automated workflow tools or through code elements and configurations as part of web-based self-help solutions.

Any service requests that impact CIs in the live environment are authorized through change management, typically as standard changes.

6.5.6 Request closure

Fulfilled service requests are referred back to the service desk for closure. Having checked that the user is satisfied with the outcome, the service desk also ensures that any financial requirements are complete, confirms that the request categorization was correct (or if not, corrects it), carries out a user satisfaction survey, chases any outstanding documentation, and formally closes the request.

6.6 Triggers, inputs, outputs and interfaces

The trigger for request fulfilment is the user submitting a service request, either via the service desk or using a self-help facility

Inputs include:

- Work requests
- Authorization forms
- Service requests
- RFCs
- Requests from various sources such as phone calls, web interfaces or email
- Requests for information.

Outputs include:

- Authorized or rejected service requests
- Request fulfilment status reports
- Fulfilled service requests
- Incidents (rerouted)
- RFCs and standard changes
- Asset and CI updates
- Updated request records.

The primary interfaces are concerned with requesting services and their subsequent deployment:

- Financial management for IT services
- Service catalogue management
- Release and deployment management
- Service asset and configuration management
- Change management
- Incident and problem management
- Access management

6.7 Information management

Request fulfilment is dependent on information from the following sources:

- RFCs
- Service portfolio
- Security policies
- Authorized approvers

Service requests contain information about which service is being asked for, who requested and authorized it, the process used to fulfil the request, the assignee and any actions, date and time of logging, and subsequent actions and closure details.

6.8 Critical success factors and key performance indicators

- CSF Requests must be fulfilled in an efficient and timely manner that is aligned to agreed service level targets for each type of request:
 - o KPI The mean elapsed time for handling each type of service request
 - o KPI The number and percentage of service requests completed within agreed target times
 - o KPI Breakdown of service requests at each stage (e.g. logged, work in progress, closed)
 - o KPI Percentage of service requests closed by the service desk without reference to other levels of support (often referred to as 'first point of contact')
 - o KPI Number and percentage of service requests resolved remotely or through automation, without the need for a visit
 - o KPI Total numbers of requests (as a control measure)
 - o KPI The average cost per type of service request

- CSF Only authorized requests are fulfilled:
 - o KPI Percentage of service requests fulfilled that were appropriately authorized
 - o KPI Number of incidents related to security threats from request fulfilment activities
- CSF User satisfaction must be maintained:
 - o KPI Level of user satisfaction with the handling of service requests (as measured in some form of satisfaction survey)
 - o KPI Total number of incidents related to request fulfilment activities
 - o KPI Size of the current backlog of outstanding service requests.

6.9 Challenges and risks

Challenges include:

- Clearly defining the type of requests to be handled by the request fulfilment process
- Establishing self-help capabilities at the front end that allow the users to interface successfully with the request fulfilment process
- Agreeing and establishing service level targets
- Agreeing the costs for fulfilling requests
- Putting in place agreements for which services are standardized and who is authorized to request them
- Making information easily accessible about which requests are available
- Making requests follow a predefined standard fulfilment procedure
- The high impact of request fulfilment on user satisfaction.

Risks include:

- Poorly defined scope, where people are unclear about what the process is expected to handle
- Poorly designed or implemented user interfaces, meaning that users have difficulty raising requests
- Badly designed or operated back-end fulfilment processes that are incapable of dealing with the volume or nature of the requests
- Inadequate monitoring capabilities, meaning that accurate metrics cannot be gathered.

6.10 Roles and responsibilities

6.10.1 Request fulfilment process owner

- Carrying out the generic process owner role for the request fulfilment process
- Designing request fulfilment models and workflows
- Working with other process owners to ensure there is an integrated approach across request fulfilment, incident management, event management, access management and problem management.

6.10.2 Request fulfilment process manager

- Carrying out the generic process manager role for the request fulfilment process
- Planning and managing support for request fulfilment tools and processes, and coordinating interfaces with other service management processes
- Assisting with identification of suitable staffing levels to deliver request fulfilment activities and services
- Ensuring all authorized service requests are being fulfilled on a timely basis, in line with service level targets
- Representing request fulfilment activities at change advisory board (CAB) meetings
- Overseeing feedback from customers and reviewing request fulfilment activities for consistency, accuracy and effectiveness in order to proactively seek improvements.

6.10.3 Request fulfilment analyst

- Providing a single point of contact and end-to-end responsibility to ensure submitted service requests have been processed
- Providing an initial triage of service requests to determine which IT resources will be engaged to fulfil them
- Communicating service requests to other IT resources that will be involved in fulfilling them
- Escalating service requests in line with established service level targets
- Ensuring service requests are appropriately logged.

7 Change evaluation

7.1 Purpose and objectives

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. The objectives of change evaluation are to:

- 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 many 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.

7.2 Scope

Every change must be authorized by a suitable change authority at various points in its lifecycle; for example, before build and test, before it is checked into the definitive media library (DML), and before it is deployed to the live environment. Evaluation is required before each of these authorizations, to provide the change authority with advice and guidance.

This 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 is normally documented in the change models used to manage each type of change.

7.3 Value to the business

Change evaluation is, by its very nature, concerned with value. Specifically, effective change evaluation establishes the use made of resources in terms of delivered benefit, and this information allows a more accurate focus on value in future service development and change management

7.4 Policies, principles and basic concepts

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

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.

7.5 Process activities, methods and techniques

7.5.1 Evaluation plan

Change evaluation is carried out from several different perspectives to help identify unintended as well as intended effects.

7.5.2 Understanding intended and unintended effects of a change

The SDP is analyzed to understand the change and the expected benefits. Documentation should make the intended effects clear and include specific measures to determine the effectiveness of the change.

Unintended effects of the change must be identified wherever possible. This may involve discussions with stakeholders and attempts to understand the full impact of the change

7.5.3 Evaluation of predicted and actual performance

A risk assessment is carried out, based on customer requirements (including acceptance criteria) and predicted performance. If this risk assessment shows unacceptable risks, then an interim evaluation report is created to warn change management, and evaluation activity stops until change management makes a decision.

After the change has been implemented, a report on actual performance is received from operations staff (or early life support) and another risk assessment is carried out. If this risk assessment shows unacceptable risks, then an interim evaluation report is created to warn change management, and evaluation activity stops until change management makes a decision.

If risks are acceptable, then no interim evaluation report is produced and further analysis is carried out to create an evaluation report. This contains:

- Deviations report
- Risk profile
- Qualification statement or validation statement (if appropriate)
- Recommendation

7.6 Triggers, inputs, outputs and interfaces

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

Inputs include:

- SDP, including service charter and service acceptance criteria
- Change proposal
- RFC, change record and detailed change documentation
- Discussions with stakeholders
- Test results and report.

Outputs are:

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

Interfaces:

- Change management
- Service design package
- Service level management or business relationship management
- Service validation and testing process

7.7 Information management

Much of the information required for change evaluation should be available from the service knowledge management system (SKMS). All evaluation reports should be checked into the CMS and soft-copy versions of the reports stored in the SKMS.

7.8 Critical success factors and key performance indicators

- CSF Stakeholders have a good understanding of the expected performance of new and changed services:
 - KPI Reduced number of incidents for new or changed services caused by failure to deliver expected utility or warranty
 - KPI Increased stakeholder satisfaction with new or changed services as measured in customer surveys
- CSF Change management has good-quality evaluations to help make correct decisions:
 - KPI Increased percentage of evaluations delivered by agreed times
 - KPI Reduced number of changes that have to be backed out due to unexpected errors or failures.

7.9 Challenges and risks

Challenges include:

- Developing standard performance measures and measurement methods
- Inaccuracy of information supplied by suppliers and projects
- Understanding different stakeholder perspectives
- Managing risk as it affects the overall organization, communicating the approach to risk, and encouraging a risk management culture
- Measuring variation in predictions during and after transition and demonstrating improvement.

Risks include:

- Lack of clear criteria for when change evaluation is 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.

7.10 Roles and responsibilities

7.10.1 Change evaluation process owner

- Carrying out the generic process owner role for the change evaluation process
- Working with other process owners to ensure that there is an integrated approach to service management.

7.10.2 Change evaluation process manager

- Carrying out the generic process manager role for the change evaluation process
- Planning and coordinating all resources needed to evaluate changes
- Ensuring that change evaluation delivers evaluation reports and interim evaluation reports in time to ensure that change authorities are able to use them to support their decision-making.

7.10.3 Change evaluation practitioner

- Using the service design and the release package to develop an evaluation plan as input to service validation and testing
- Establishing risks and issues associated with all aspects of the service transition (for example, through risk workshops)
- Creating an evaluation report as input to change management.

8 Knowledge management

8.1 Purpose and objectives

The purpose of knowledge management is to enable organizations to improve the quality of decision-making by ensuring that reliable and secure information and data are available. The objectives of knowledge management are to:

- Improve the quality of management decision-making by ensuring that reliable and secure knowledge, information and data are available throughout the service lifecycle.
- Enable the service provider to be more efficient and improve the quality of the service; increase satisfaction; and reduce the cost of the service by obviating the need to rediscover knowledge.
- Ensure that staff has 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.
- Maintain a service knowledge management system (SKMS) that provides controlled access to knowledge, information and data that is appropriate for each audience.
- Gather, analyze, store, share, use and maintain knowledge, information and data throughout the service provider organization.

8.2 Scope

The scope of knowledge management extends across the lifecycle and is referenced throughout ITIL. It includes oversight of the management of knowledge, and the information and data from which that knowledge is derived.

The scope of knowledge management does not include the capture, maintenance and use of service asset configuration data. These activities remain under the control and management of service asset and configuration management.

8.3 Value to the business

Knowledge management is especially significant within service transition. Effective knowledge management is a powerful asset for all roles across the service lifecycle.

Implementation of an SKMS helps reduce the cost of maintaining and managing services by increasing the efficiency of operational procedures and reducing risks that arise from the lack of proper mechanisms

8.4 Policies, principles and basic concepts

8.4.1 Knowledge management policies

Knowledge management policies are required to guide all staff in the behaviors needed to make it effective. Policy statements will be very dependent on the culture of the organization, but typically might include the following:

- The knowledge and information needed to support the services must 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 must be created, reviewed, approved, maintained, controlled and disposed of following a formal documented process.

8.4.2 Data-to-Information-to-Knowledge-to-Wisdom structure

- **Data.** Is facts about events. Most organizations capture massive amounts of data, some of which is stored in structured databases, such as service management, configuration management system (CMS) and databases.
- **Information.** Comes from providing a context to data. Information is typically stored in semi-structured formats such as in documents, spreadsheets and email. Knowledge management facilitates capture, query, finding, re-using and learning from information, so that mistakes are not repeated and work is not duplicated.
- **Knowledge.** Is composed of tacit experiences, ideas and insights, values and judgments of individuals. People gain knowledge both from their own expertise and that of their peers as well as from the analysis of information and data. Knowledge is dynamic and context-based. Knowledge transforms information into a format that is easy to use. This is achieved by use of previously collected experiences, awareness and anticipation.
- **Wisdom.** Uses application and contextual awareness to provide judgment.

8.4.3 The service knowledge management system

Specifically within IT service management, knowledge management is focused within the SKMS. Underpinning this knowledge is a considerable quantity of data and information, held in the CMS.

8.5 Process activities, methods and techniques

8.5.1 Knowledge management strategy

There should be as wide a span as practicable for knowledge management to incorporate anyone likely to be able to contribute to or benefit from knowledge management.

Specifically, knowledge management identifies and plans for the capture of relevant knowledge and the information and data that support it.

8.5.2 Knowledge transfer

The challenge is transferring knowledge between parts of the organization. The knowledge needs to be in a form that is both applicable and easy to use.

If necessary, a gap analysis of knowledge transfer is undertaken. The output is a communications improvement plan, which recognizes that people receive and interpret knowledge in different ways, using different learning styles.

8.5.3 Managing data, information and knowledge

Knowledge rests on the management of the information and data that underpin it. To be efficient, this process needs to have an understanding of some key process inputs such as:

- What data is available
- The cost of capturing and maintaining data
- The value of that data
- How the data and information will be used
- Applicable policies, legislation, standards and other requirements
- Intellectual property and copyright issues.

In order to make effective use of data in terms of delivering knowledge, it is essential to have a relevant architecture matched to the organization and the knowledge requirements.

Once the requirements have been defined and the architecture set up, data and information management requirements can be established to support knowledge management

As with all ITIL processes and functions, the capture and use of data and information to support knowledge management needs regular review and attention for continual improvement.

Implementation of an SKMS helps reduce the costs of maintaining and managing services. It does this by increasing the efficiency of operational mechanisms while reducing the risks that may be caused by inaccurate or ineffective mechanisms. Useful materials may include:

- Training materials
- Business process documentation
- Process maps
- Known errors and workarounds
- Business and public calendars.

8.6 Triggers, inputs, outputs and interfaces

Knowledge management has many triggers, relating to every requirement for storing, maintaining or using knowledge, information or data within the organization.

Inputs to knowledge management include all knowledge, information and data used by the service provider, as well as relevant business data.

The key output of knowledge management is the knowledge required to make decisions and to manage the IT services; this is maintained within an SKMS.

Knowledge management has interfaces with every other service management process in every stage of the lifecycle.

8.7 Information management

There is no simple answer to the question, 'What tools and systems are needed to support knowledge management?' In practice, an SKMS is likely to consist of a large number of tools and repositories, some running independently and others having links between them to allow cross-referencing and creation of added value.

8.8 Critical success factors and key performance indicators

- CSF Availability of knowledge and information that helps to support management decision-making:
 - KPI Increased number of accesses to the SKMS by managers
 - KPI Increased percentage of SKMS searches by managers that receive a rating of 'good'
- CSF Reduced time and effort required to support and maintain services:
 - KPI Increased number of times that material is re-used in documentation such as procedures, test design and service desk scripts
 - KPI Increased number of accesses to the SKMS by service operation teams
 - KPI Reduced transfer of issues to other people and more resolution at lower staff levels.

8.9 Challenges and risks

The challenge is to help all the stakeholders understand the added value that a more holistic approach to knowledge management can bring, and to continue to demonstrate this value as an SKMS is built. The risks to knowledge management include:

- Focusing on the supporting tools, rather than on the creation of value
- Insufficient understanding of what knowledge, information and data are needed by the organization
- Lack of investment in the tools and people needed to support the SKMS
- Spending too much effort on knowledge capture while paying insufficient attention to knowledge transfer and re-use
- Storing and sharing knowledge and information that are not up to date and relevant
- Lack of support and commitment from stakeholders.

8.10 Relationship with continual service improvement

Knowledge management plays a key role in continual service improvement. Each phase of the lifecycle captures data to gain knowledge and understanding, which in turn leads to wisdom. This is frequently referred to as the DIKW model

8.11 Roles and responsibilities

8.11.1 Knowledge management process owner

- Carrying out the generic process owner role for the knowledge management process

- Creating the overall architecture for identification, capture and maintenance of knowledge within the organization.

8.11.2 Knowledge management process manager

- Carrying out the generic process manager role for the knowledge management process (see section 1.5)
- Ensuring that all knowledge items can be accessed in an efficient and effective manner by those who need them
- Planning and managing support for knowledge management tools and processes
- Encouraging people throughout the service provider organization to contribute knowledge to the SKMS
- Acting as an adviser to business and IT personnel on knowledge management matters, including policy decisions on storage, value and worth.

8.11.3 Knowledge management process practitioner

- Identifying, controlling and storing any information deemed to be pertinent to the services provided that is not available by other means
- Maintaining controlled knowledge items to ensure that they are current, relevant and valid
- Monitoring publicity regarding the knowledge information to ensure that information is not duplicated and is recognized as the central source.

The person carrying out this role is recognized as a central source of information and in some organizations is called a 'knowledge librarian'.

8.11.4 Knowledge creator

Creation and sharing of knowledge is often written into the job descriptions of people in many different roles within IT and the business.

9 Technology and implementation

9.1 Generic requirements for IT service management technology

The same technology should be used at all stages of the service lifecycle. Generally this includes:

- Self-help
- Workflow or process engine
- Integrated configuration management system (CMS)
- Discovery, deployment and licensing technology
- Remote control
- Diagnostic utilities
- Reporting
- Dashboards
- Integration with business service management

9.2 Evaluation criteria for technology and tools

Some generic points that organizations should consider when selecting any service management tool include:

- Data handling, integration, import, export and conversion
- Data backup, control and security
- Ability to integrate multi-vendor components, existing and into the future
- Conformity with international open standards
- Usability, scalability and flexibility of implementation and usage
- Support options provided by the vendor, and credibility of the vendor and tool
- The platform the tool will run on and how this fits the IT strategy
- Training and other requirements for customizing, deploying and using the tool
- Costs: initial and ongoing.

It is generally best to select a fully integrated tool, but this must support the processes used by the organization, and extensive tool customization should be avoided.

Tool requirements should be categorized using MoSCoW analysis:

- M – MUST have this
- S – SHOULD have this if at all possible
- C – COULD have this if it does not affect anything else
- W – WON'T have this, but WOULD like in the future.

9.3 Practices for process implementation

9.3.1 Managing change in service operation

Service operation staff must be involved in assessment of all changes, not just as members of the change advisory board (CAB) but at a sufficiently early stage that they can influence design decisions.

The measure of success for any change made to service operation is that customers do not experience any variation or outage. The effects should be invisible, apart from enhanced functionality, quality or financial savings resulting from the change.

9.3.2 Service operation and project management

It is important that all projects make use of project management processes. Using project management processes can bring the following benefits:

- Project benefits are agreed and documented
- It is easier to see what is being done and how it is being managed
- Funding can be easier to obtain
- There is greater consistency and improved quality
- Objectives are more likely to be achieved, leading to higher credibility for operational groups.

9.3.3 Assessing and managing risk in service operation

Risk assessment and management is required throughout the service lifecycle.

- Risks from potential changes or known errors
- Failures or potential failures: these may be identified by event management, incident management or problem management, but also by warnings from manufacturers, suppliers or contractors
- Environmental risks: risks to the physical environment as well as political, commercial or industrial relations risks, which could lead to invoking IT service continuity
- Suppliers, particularly if they control key service components
- Security risks
- Support of new customers or services.

9.3.4 Operational staff in service design and transition

Activities during service design and service transition should involve staff from all IT groups to ensure that new components and services are designed, tested and implemented in a way that will provide the service utility and service warranty required.

Service operation staff must be involved during the early stages of design and transition to ensure that new services are fit for purpose from an operational perspective and supportable in the future. This will mean that:

- Services are capable of being supported from a technical and operational viewpoint with existing (or agreed additional) resources and skills
- There is no adverse impact on other practices, processes or schedules
- There are no unexpected operational costs
- There are no unexpected contractual or legal complications
- There are no complex support paths with multiple support departments or third parties.

9.4 Challenges, critical success factors and risks relating to implementing practices and processes

9.4.1 Challenges

- Enabling almost every business process and service in IT, resulting in a large customer and stakeholder group that is involved and impacted by service transition
- Managing many contacts, interfaces and relationships through service transition, including a variety of different customers, users, programmes, projects, suppliers and partners. Establishing 'Who is doing what, when and where?' and 'Who should be doing what, when and where?'
- Little harmonization and integration of the processes and disciplines that impact service transition, such as finance, engineering and human resource management
- Inherent differences among the legacy systems, new technology and human elements that result in unknown dependencies and are risky to change
- Achieving a balance between maintaining a stable live environment and being responsive to the business needs for changing the services
- Achieving a balance between pragmatism and bureaucracy
- Understanding the different stakeholder perspectives that underpin effective risk management within an organization.

9.4.2 Critical success factors

- Understanding and managing the different stakeholder perspectives that underpin effective risk management within an organization, and establishing and maintaining stakeholder buy-in and commitment
- Having clearly defined relationships and interfaces with programme and project management
- Integrating with the other service lifecycle stages, processes and disciplines that impact service transition
- Automating processes to eliminate errors and reduce the cycle time
- Creating and maintaining new and updated knowledge in a form that people can find and use
- Being able to understand the service and technical configurations and their dependencies
- Demonstrating improved cycle time to deliver change with fewer variations in time, cost and quality predictions during and after transition

- Demonstrating that the benefits of establishing and improving the service transition practice and processes outweigh the costs (across the organization and services).

9.4.3 Risks

- Change in accountabilities, responsibilities and practices of existing projects that demotivate 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.

Other implementation risks include:

- Excessive costs to the business generated by overly risk-averse service transition practices and plans
- Knowledge sharing (the wrong people may have access to information)
- Lack of maturity and integration of systems and tools, resulting in people 'blaming' technology for other shortcomings
- Poor integration between the processes, causing process isolation and a silo approach to delivering ITSM
- Loss of productive hours, higher costs, loss of revenue or perhaps even business failure as a result of poor service transition processes.

9.5 Planning and implementing service management technologies

There are a number of factors to consider when deploying and implementing ITSM support tools:

- Licenses
 - Dedicated licenses
 - Shared licenses
 - Web licenses
 - Service on demand
- Deployment
- Capacity checks
- Timing of technology deployment
- Type of introduction

9.6 Technology for implementing collaboration, configuration management and knowledge management

9.6.1 Collaboration

Collaboration is sharing tacit knowledge and working together to achieve goals. Typical tools to support this include:

- Shared calendars and tasks
- Threaded discussions

- Email and instant messaging
- Whiteboarding, videoconferencing and teleconferencing.
- Communities
 - Community portals
 - Email alias management
 - Focus groups
 - Repository for intellectual property, best practices and work examples
 - Online events and net shows

Workflow management provides support for managing knowledge through a predefined workflow. Tools to support this typically provide:

- Workflow design
- Routeing objects and event services
- Gatekeeping at authorization checkpoints and state transition services.

9.6.2 Configuration management system

The CMS contains details about the attributes and history of each CI, and details of the important relationships between CIs. Ideally it should be linked to the definitive media library (DML); if this is not possible, then consider automating the comparison of CMS and DML.

The CMS should prevent unauthorized changes to the infrastructure or services. All changes should be recorded, and the status of CIs should be updated automatically if possible. Features that a CMS should provide include:

- Appropriate security controls, only allowing access that is required
- Support for complex CIs with hierarchic and networked relationships and automatic update of version when a component version changes
- Easy addition, modification and deletion of CIs, with automatic validation of input data, automatic detection of relationships where possible, and maintenance of history of all CIs
- Support for model numbers, version numbers and copy numbers
- Support for baselines
- Automatic identification of related CIs when managing incidents, problems and changes
- Good interrogation and reporting, including trend analysis and graphical representation of relationships.

9.6.3 Knowledge management tools

- Document management
- Records management
- Content management
 - Web publishing tools, including conferencing, wikis and blogs
 - Word processing, flowcharting and presentation tools
 - Data and financial analysis

- Publication and distribution
- Content management systems (codifying, organizing, version control, document architectures).

9.7 The Deming Cycle

The Deming Cycle is a four-stage cycle for quality improvement:

- Plan
- Do
- Check
- Act