PRM-IT V3 Reference Library - A5 Transition

PRM-IT Version 3.0

April, 2008

PRM - IT
IBM Process Reference Model for IT

Sequencing the DNA of IT Management

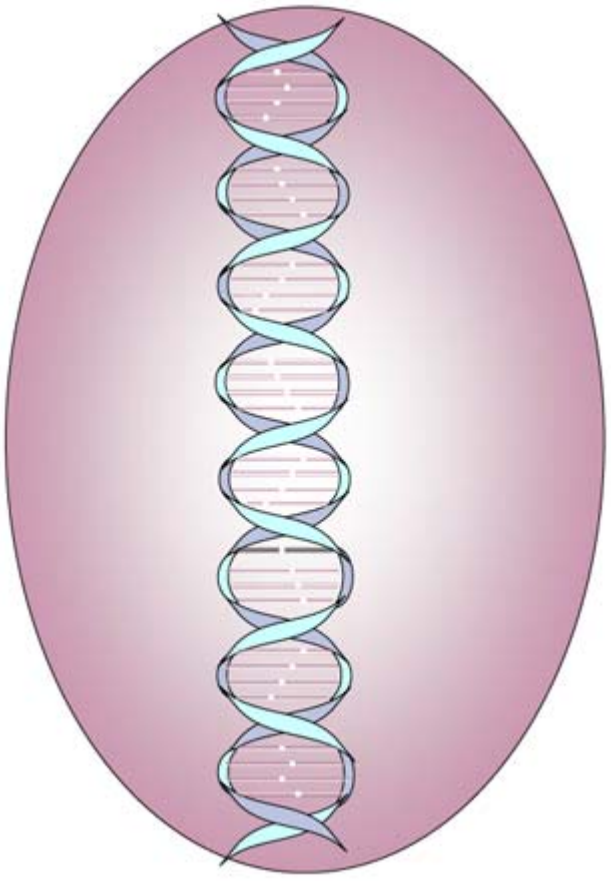

Table of Contents

Preface

The IBM Process Reference Model for Information Technology (PRM-IT) is a generic representation of the processes involved across the complete IT management domain. It contains a foundational examination of the IT process topic. It is for this reason the graphical image of the DNA double helix over the basic building block of a cell is used.

About this book

This is the seventh book in the PRM-IT Reference Library. As a reference manual, this book provides the complete description of all aspects of the process category.

Each reference manual begins with a summarization of the category, and then further considers each process in turn and the activities within each process.

Details are provided for:

- The definition of each activity
- Each control, input and output
- The sources and destinations of each control, input, and output (thereby showing the model linkages)

The full IDEF0 diagram for each category and each process is included.

The final page is a breakdown of the PRM-IT node tree for this category.

The PRM-IT Reference Library books

The PRM-IT Reference Library consists of thirteen books. The first book is the *General Information Manual*, it is a brief examination of the subject of IT processes, and provides a tour of the model.

The nine reference manuals are A0 through A8. The *A0 Manage IT* book examines the context of the processes for IT, exploring the key external agents — stakeholders and their interactions with IT. The reference manuals A1 through A8 provide the complete description of all spects of the process categories.

The reference manual *IDEFØ Diagrams* presents the full model in IDEFØ notation, and *IDEFØ Node Tree* shows the ordered list of process categories, processes, and activities.

The final book, the *Glossary*, contains the definition of every process interface object for the model and provides references to where the objects are used.

PRM-IT Reference Library	
■ General Information	■ A6 Operations
■ A0 Manage IT	■ A7 Resilience
■ A1 Governance and Management System	■ A8 Administration
■ A2 Customer Relationships	■ IDEFØ Node Tree
■ A3 Direction	■ IDEFØ Diagrams
■ A4 Realization	■ PRM-IT Glossary
■ A5 Transition	

Intended audience

An understanding of the full range of the processes relevant to IT in any business is of value to those within the IT function responsible for the specification, creation, and delivery of IT services (whether at the CIO or IT executive level), and who consider the direction and overall management of IT. Or, individuals who work within any of its competencies, needing to interface with other parts of the IT value chain or value net.

Equally, the stakeholders in the business of this IT capability will benefit from greater insight into how IT serves them. This insight will enable them to better influence IT decisions and activities, to their ultimate benefit.

Next steps

PRM-IT is a powerful management tool for purposes of investigating and identifying areas for improvement. PRM-IT also provides a proven starting-point for the design and implementation of new and upgraded IT management capabilities.

IBM IT consultants, architects, and specialists in global services who, working from this common base, are equipped with a full range of methods, techniques, and tools to assist its customers achieve their purposes.

[A5] Transition

Description

Purpose

The Transition category of processes exists to support any aspect related to a life cycle status change in *solutions* and *services*. The processes provide defined and repeatable approaches to planning, effecting and recording these transitions and can be applied to all stages of the life cycle. They also serve to maintain control over the Information Technology (IT) resources that are subject to such status changes. Further, the processes in this category provide vital enabling information to other process areas related to the management of IT. Using these processes, developments in IT capabilities supporting the stakeholding businesses and customers achieve their desired operational status from which value can be derived.

Rationale

A transition can vary in scope and scale from a roll out of a major solution to a large population of users across multiple geographic territories to the installation of a fix or patch to a single configuration item or the controlled update of an individual software module during development. Transition instances can also be triggered by changes in the service provider arrangements, whether or not there is also a change in service capabilities and characteristics. Any modification to a known set of resources carries with it some risk of failure and so, whatever the motivation for the transition, there is a need to ensure that approaches which minimize that risk are followed and that information about the state of resources is maintained.

Value

- Improves the speed of innovation while balancing the business need for stability in the IT infrastructure
- Controls and maintains accurate information on the infrastructure, applications, and services
- Implements solutions that provide new functionality, eliminates the root causes of defects or performs tuning actions without business disruption
- Enables gradual and measured improvements in the way that changes are introduced into complex and interdependent live environments
- Supports the efficiency and effectiveness of other processes by providing accurate information on managed elements (configuration items (CIs), managed objects, among others)

Controls

- Architecture Baselines and Roadmaps (From: A3 A33 A334)
- IT Plan (From: A3 A36 A365)
- IT Strategy (From: A3 A31 A315)
- Service Catalog (From: A2 A23 A235)
- SLA, OLA, UCs (From: A2 A24 A243)
- IT Management Ecosystem (From: A1)
- Environment Information (From: Outside-the-Model)
- IT Budget (From: A8 A81 A813)
- Compliance Plans and Controls (From: A7 A71 A714)

Inputs

- Solution_ Accepted (From: A4 A45 A456)
- CI Requisition (From: A4 A42 A423 A424 A43 A433 A434 A44 A444)
- Solution Design (From: A4 A42 A425)
- Solution Plans and Commitments (From: A4 A41 A42 A422 A425 A43 A432 A44 A442 A45 A452)
- Project Plan (From: A3 A37 A374)
- Product Package (From: A3 A35 A353 A354 A355)
- CI Data Update Package (From: A4 A42 A424 A43 A433 A434 A435 A436 A437 A44 A444 A45 A456 A51 A516 A52 A523 A526 A53 A535 A536 A6 A63 A634 A64 A645 A65 A652 A7 A75 A753 A754)
- Underpinning Contracts (From: A8 A82 A823)
- IT Financial Reports (From: A8 A81 A813 A814 A815)
- Service Resilience Plans (From: A7)
- Service Request_ Authorized (From: A6 A61 A613)
- Change Request (From: A2 A23 A232 A3 A35 A355 A4 A42 A422 A43 A432 A44 A442 A54 A542 A6 A61 A613 A62 A621 A64 A644 A65 A655 A66 A665 A7 A72 A725 A73 A737 A74 A744 A745 A75 A752 A754 A76 A765 A766)

Outputs

- Change Schedule (To: A514 A516 A517 A52 A522 A525 A54 A543 A545 A6 A63 A632 A66 A665 A7 A74 A744 A745 A75 A752 A753)
- Solution_ Deployed (To: A3 A32 A4 A43 A433 A44 A443 A6 A62 A63 A634 A64 A641 A7 A76)
- Change Information (To: A2 A23 A233 A235 A3 A35 A355 A513 A514 A515 A516 A517 A54 A542 A543 A6 A61 A613 A615 A62 A621 A63 A632 A64 A641 A65 A654 A66 A662 A666 A7 A72 A721 A725 A73 A731 A735 A736 A74 A741 A742 A743 A75 A751 A76 A761 A764)
- Configuration Information (To: A3 A33 A336 A4 A42 A422 A423 A424 A44 A442 A443 A51 A513 A514 A516 A52 A523 A524 A53 A533 A534 A535 A545 A55 A553 A6 A61 A612 A62 A623 A63 A634 A635 A64 A642 A65 A652 A653 A654 A66 A662 A67 A674 A7 A72 A724 A726 A727 A73 A735 A736 A74 A742 A743 A744 A75 A752 A76 A764 A765 A766)
- Incident (To: A537 A6 A65 A652)
- Asset Information (To: A54 A543 A7 A71 A713 A72 A724 A8 A81 A812 A814 A815)
- Project Proposal (To: A3 A34 A342 A35 A352 A36 A364)
- Asset Deployment Items and Data (To: A4 A43 A51 A52 A522 A523 A524 A53 A534)
- CIs (To: A4 A43 A434 A44 A444)

Processes

This process category is composed of these processes:

- A51 Change Management
- A52 Release Management
- A53 Deployment Management
- A54 Configuration Management
- A55 Asset Management

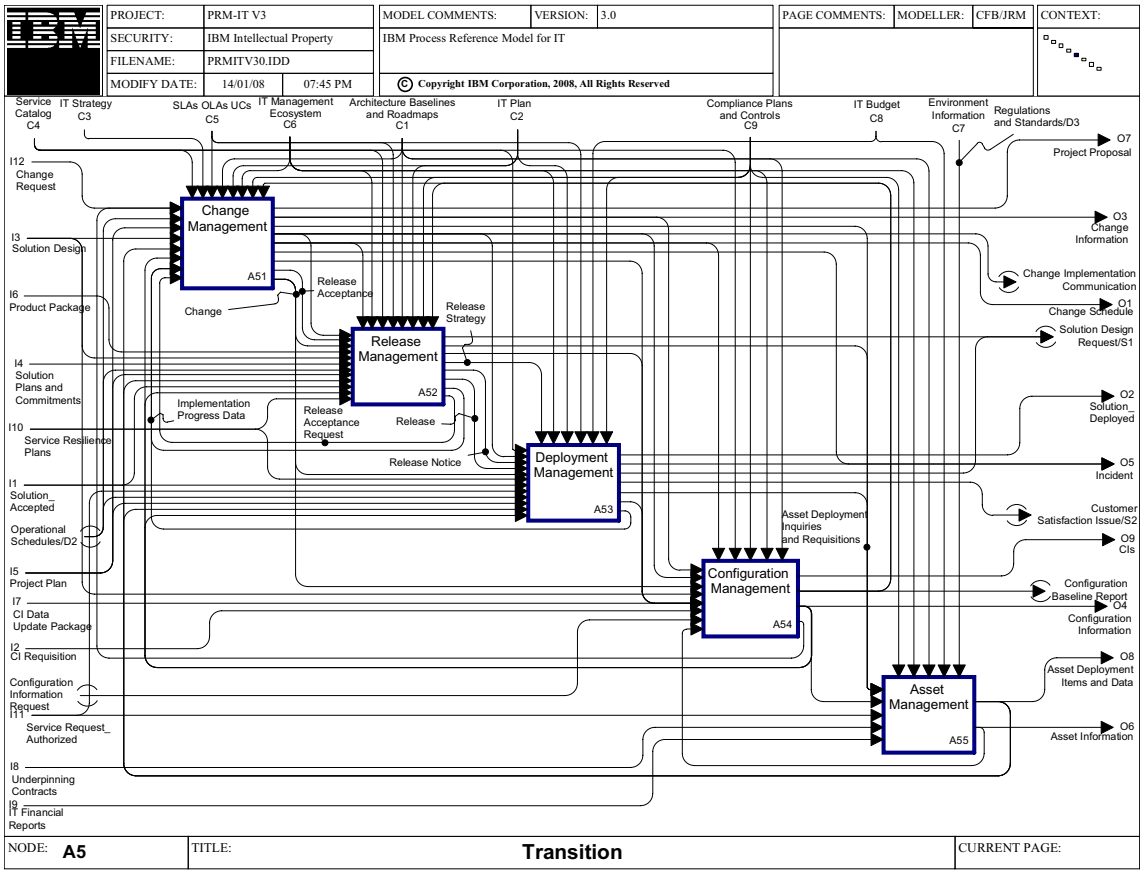

Figure 1. A5 Transition Diagram

[A51] Change Management

Purpose

The purpose of the Change Management process is to achieve the successful introduction of changes to an IT system or environment. Success is measured as a balance of the timeliness and completeness of change implementation, the cost of implementation, and the minimization of disruption caused in the target system or environment. The process also ensures that appropriate details of changes to IT resources (assets, CIs) are recorded.

Basically, a change is anything that alters the status of a configuration item (CI). This typically includes anything that adds to, deletes from, or modifies the IT environment. The definition of a change is the addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

A change request (for which RFC is an established synonym) is the means for documenting proposed change and actual change activity in IT resources or capabilities. Change requests can be triggered for a wide variety of reasons, from a wide variety of sources. Change requests can be concerned with any part of the infrastructure or with any service or activity.

Outcomes

As a result of the successful implementation of the Change Management process:

- Changes are introduced in a timely and controlled manner
- Proposed changes are not approved nor introduced without an accurate assessment of their costs and other effects
- Incidents resulting from the introduction of changes are minimized
- Service quality is measurably improved
- Appropriate balance is maintained between the business need to deploy innovation and the need to maintain the stability of IT service

Scope

Change Management typically begins with the creation of a Change Request (RFC). The change request documents details of the proposed change in order to support a range of business and technical assessments, leading to approval (or rejection) and ultimately to application of the change.

The Change Management process represents a pattern of activities and work flow, which can be implemented over a range of contexts. The most prominent contexts include operations and development. Operations Change Management and Development Change Management are similar in a number of ways, including recording of all change requests, assessment of all change requests prior to approval, a team-based approach to change approval, and review of change effectiveness. However, they are different in a number of ways:

- Development Change Management addresses changes proposed to a system under development. These changes may include requests for new functionality, patches, or redevelopment. In contrast, Operations Change Management focuses on changes to operational CIs in the entire IT infrastructure. These changes can include capacity tuning, asset transfer, and system resets.
- Changes are assessed and approved using a team. Each context typically has its own change board and membership, addressing different types of changes, and using different assessment criteria. In development, the team is often known as the Change Control Board; in ITIL, the term Change Advisory Board is used. A higher level board can be established to ensure integration of changes across contexts.

Change Management can appear in other contexts besides operations and development. There can be a single implementation of the Change Management process or several, with each implementation covering the scope of a defined context. Factors such as size of the organization and different start and end points defining a change can lead to multiple implementations of change management, with each following the process principles and pattern described but employing procedures and decision criteria customized for their context.

This process establishes classification and categorization schemes to assist with change assessment activities. It also defines the implementation approaches that will be assigned to approved changes in order to standardize the supervisory control levels, consistent with the assessment recommendations. ITIL, in the context of managing production environments, uses the term Change Model for these schemes.

Definition of Change Model: “A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a Change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software Release).”[1]

Examples of change models:

- A standard change is “A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request.”[2]
- An emergency change is “A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch.”[3]
- For software development, there will frequently be different change types based on the impact to the overall system, and hence requiring different levels of approval, such as architectural change as compared with scope change, and change that is local to one component.

Some activities in the process require examination of several or all changes collectively rather than on an individual basis. For example, scheduling changes for implementation requires consideration of the other changes planned for the same dates and target environments in order to identify conflicts.

Includes

- Planned changes, standard changes (pre-approved by policy), and emergency changes (policy exception request)
- Establishing both recurring and one-time only schedules (change windows) during which changes can be performed without negatively affecting commitments, such as project schedules, projected availability, or SLA commitments
- Enforcement of standard methods and procedures from request for change through post implementation review
- Establishing regular meetings and communication schedules to evaluate proposed changes and schedules
- Control and management coordination of the implementation of those changes that are subsequently approved

1. ITIL V3 Glossary
2. ITIL V3 Glossary
3. ITIL V3 Glossary

- Maintenance of open channels of communications to promote smooth transition when changes take place
- Increased visibility and communication of changes to both business and support staff

Excludes

- Requirements Management (Stakeholder Requirements Management)
- Creation of new or revised functionality (Realization category processes)
- Building the packaging for the delivery of new or revised functionality (Release Management)
- Technical implementation, such as distribution, preparation, installation, and back out if necessary (Deployment Management)
- Configuration Management, although the interface to this process must be managed
- Asset Management, although the interface to this process must be managed
- Business transformation and organizational change (IT Customer Transformation Management)

Controls

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[4]

- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs)

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the

4. ITIL V3 Glossary

responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers."[5]

- OLA: "An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties."[6]
- UC: "A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[7]

These agreements can be in a draft or finalized status.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

Inputs

- Change Request (From: A2 A23 A232 A3 A35 A355 A4 A42 A422 A43 A432 A44 A442 A54 A542 A6 A61 A613 A62 A621 A64 A644 A65 A655 A66 A665 A7 A72 A725 A73 A737 A74 A744 A745 A75 A752 A754 A76 A765 A766)

  Change requests (also known as RFCs) are the means for submitting proposed change and actual change activity in the environment. Change requests can be triggered for a wide variety of reasons, from a broad spectrum of sources. They can be concerned with any part of the environment or with any service or activity.

5. ITIL V3 Glossary
6. ITIL V3 Glossary
7. ITIL V3 Glossary

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

- Solution Design (From: A4 A42 A425)

  Solution design, including *conceptual*, *macro*, and *micro* designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Implementation Progress Data (From: A375 A52 A523 A524 A53 A535 A536 A635)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Release Acceptance Request (From: A52 A524)

  A request for final approval from Change Management for a release to be able to proceed to rollout. The request will be accompanied by evidence of the release having passed its acceptance criteria.

Outputs

- Project Proposal (To: A3 A34 A342 A35 A352 A36 A364)

  A formal statement of an idea being put forward for consideration that includes the business case for the proposed IT investment.

- Change Information (To: A2 A23 A233 A235 A3 A35 A355 A513 A514 A515 A516 A517 A54 A542 A543 A6 A61 A613 A615 A62 A621 A63 A632 A64 A641 A65 A654 A66 A662 A666 A7 A72 A721 A725 A73 A731 A735 A736 A74 A741 A742 A743 A75 A751 A76 A761 A764)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Change Implementation Communication (To: A375 A52 A522 A523 A524 A53 A535 A536 A54 A542 A543 A635 A655 A665)

  Information used to coordinate and implement a change.It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Change Schedule (To: A514 A516 A517 A52 A522 A525 A54 A543 A545 A6 A63 A632 A66 A665 A7 A74 A744 A745 A75 A752 A753)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.” [8]

- Incident (To: A537 A6 A65 A652)

  A fault in IT service and infrastructure that has been reported, or an event that could cause an interruption to one or more services. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a service request and becomes an incident once it is determined that a fault is being reported.

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- Release Acceptance (To: A52 A524 A525)

  The notification of approval that the *release* can proceed to its rollout activities.

- Change (To: A412 A516 A517 A518 A52 A522 A53 A532 A54 A543 A753)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

Activities

This process is composed of these activities:

- A511 Establish Change Management Framework
- A512 Create and Record Change Request
- A513 Accept and Categorize Change
- A514 Assess Change
- A515 Authorize and Schedule Change
- A516 Coordinate Change Implementation
- A517 Review and Close Change
- A518 Monitor and Report Change Management
- A519 Evaluate Change Management Performance

8. ITIL V3 Glossary

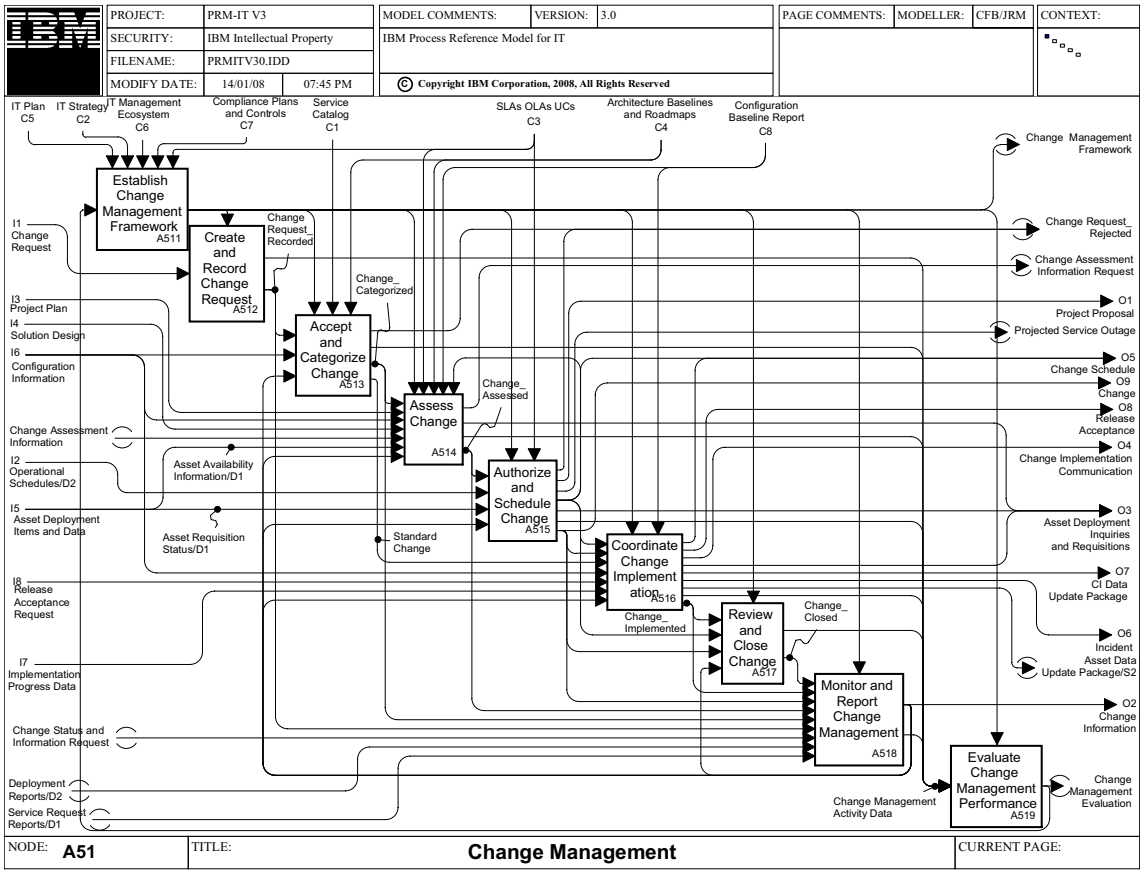

Figure 2. A51 Change Management

[A511] Establish Change Management Framework

Description

This activity defines the way Change Management will be managed and controlled. It defines the rules by which Changes can be allowed to flow through the Change Management Process, and takes into account other functions that will be affected by the Change Management process, such as Configuration Management.

This activity facilitates the creation of a Change Management Framework, which is essential in ensuring that changes that are introduced to a live environment are done so with mitigated risk, and with minimal or no disruption.

- It creates and maintains the scope, policies, standards, responsibilities, and procedures of the Change Management process. This includes defining change models, determining relationships with other processes, change request specifications, and the composition of the change advisory board (CAB).
- It also carries out the assignment of roles and responsibilities.

This is not a one-off activity. It should be undertaken periodically to ensure that the framework remains suitable for the business, and it should take into account changes to the size of the organization, service levels, business, IT strategies, and operational plans.

Controls

- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.

- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs)

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[9]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[10]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[11]

  These agreements can be in a draft or finalized status.

9. ITIL V3 Glossary
10. ITIL V3 Glossary

Inputs

- Change Management Evaluation (From: A519)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

Outputs

- Change Management Framework (To: A233 A234 A512 A513 A514 A515 A516 A517 A518 A519 A611 A641)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

[A512] Create and Record Change Request

Description

The activity of formulating and storing the information about any proposed or after-the-fact change. The request will contain a defined outline of informational sections which have been established as necessary in order for it to be progressed into assessment and the further activities of Change Management. Information can vary depending upon the context, scale, and potential impact of the requested change.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

Inputs

- Change Request (From: A2 A23 A232 A3 A35 A355 A4 A42 A422 A43 A432 A44 A442 A54 A542 A6 A61 A613 A62 A621 A64 A644 A65 A655 A66 A665 A7 A72 A725 A73 A737 A74 A744 A745 A75 A752 A754 A76 A765 A766)

  Change requests (also known as RFCs) are the means for submitting proposed change and actual change activity in the environment. Change requests can be triggered for a wide variety of reasons, from a broad spectrum of sources. They can be concerned with any part of the environment or with any service or activity.

Outputs

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change Request_ Recorded (To: A513 A518)

  The details of a change request, captured in a document or other format defined by the Change Management Framework.

11. ITIL V3 Glossary

[A513] Accept and Categorize Change

Description

This activity begins with the examination of the change request to determine if it can be accepted for consideration. To accept a change request all required information must be logged; omitted or incomplete information can cause a change request to be returned. The return of the change request will usually indicate that the request can be re-submitted if the missing or inadequate information is provided. After initial acceptance, the change request is categorized. Categorizing consists of identifying whether the change request fits categories such as:

- Standard change typically pre-approved
- Normal change requiring control using the designed, preferred Change Management process and procedures
- Exception change (such as an emergency change) requiring Change Management control but under non-preferred circumstances

ITIL suggests that each categorization can have an associated change model, defined as: “A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a Change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software Release).”[12]

Finally, the change request is assigned to the appropriate roles, functions or teams, to evaluate the change.

- Change requests that are out of scope or not within policy are rejected. In these cases, the submitter might be guided to present their request as a new requirement.
- Standard changes are sent for implementation.
- The remaining change requests are marked for assessment, and routed according to their content and categorization.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.
- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[13]
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

12. ITIL V3 Glossary
13. ITIL V3 Glossary

Inputs

- Change Request_ Recorded (From: A512)

  The details of a change request, captured in a document or other format defined by the Change Management Framework.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

Outputs

- Change Request_ Rejected

  Any change request which has been rejected, and sent back to the requestor. Reasons for rejection include:

  - Lack of authorization or funding
  - The change requested is beyond the scope of Change Management (for example, it is a new requirement)
  - The change request is incomplete or in error
  - The change request has been assessed as having too high a risk and needs rework

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change_ Categorized (To: A514 A518)

  The change request, which has completed acceptance, is now recognized as a *change.* The categorization indicates the types and levels of assessment needed.

- Standard Change (To: A516)

  Those changes that have been pre-approved for deployment. They include well known and proven tasks, and have limited (and well understood) or no impact on the integrity of the target context, such as the infrastructure. These changes will also have all entitlement issues, like financial approvals, and licensing already resolved.

  Implementation can be either user-driven or managed by the IT function. Examples include:

  - Installation of printer drivers from a pre-installed library on a PC
  - Downloading and installation of software or fixes from vendor sites
  - Upgrading a laptop to a larger hard drive

[A514] Assess Change

Description

This activity analyzes each change to determine its impact on existing and planned CIs as well as the impact on resources required to build and deploy the change. This involves identifying the appropriate change model for handling the change, scheduling a CAB meeting if specified by the change model, and obtaining a complete set of analysis results and issues.

In this activity, the impact of a change is evaluated from both the IT and business perspectives, ensuring that the change can be successfully implemented with a minimal impact to committed services and still meet business requirements.

This activity allocates priority based on urgency, and if the change is for the resolution of a problem, the priority will also reflect projected impact. Assessment often assigns impact categorization classes such as *minor*, *significant*, or *major*.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[14]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[15]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[16]

  These agreements can be in a draft or finalized status.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

14. ITIL V3 Glossary
15. ITIL V3 Glossary
16. ITIL V3 Glossary

- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[17]

Inputs

- Change_ Categorized (From: A513)

  The change request, which has completed acceptance, is now recognized as a change. The categorization indicates the types and levels of assessment needed.

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- Change Assessment Information

  Any information about the potential impact or risks relating to a change, including input from the business and from any other relevant process within IT.

- Asset Availability Information (From: A552)

  Details of the ability of the subject IT asset or assets to be made available for deployment or development use. The details will include:

  - Quantities
  - Specifications
  - Dates
  - Locations.

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

Outputs

- Request for Change Assessment Information Request

  A request to any relevant party to provide information that will contribute to the assessment of a change.

17. ITIL V3 Glossary

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change_ Assessed (To: A515 A518)

  The change, including the collection of assessment recommendations.

[A515] Authorize and Schedule Change

Description

This activity represents a decision checkpoint against the change based on impact. It examines the analysis results from Assess Change and determines whether to approve the change.

If approved, the change deployment approach and targeted change deployment schedule are determined for the change. Approval types can include financial, technical, and business, all of which can be considered by any body approving the change. The manner in which the change is approved will depend on the organization structure, but formal approval will be obtained for each change from the change authority (CA). This can be Change Management, Service Management, or some other nominated person or group.

If a solution does not exist, one can be requested (through Project Proposal) before the change is approved. If a solution does exist, a change can then be scheduled.

The activity for scheduling a change takes into account the Change Schedule, eliminating conflict between differing changes, and assigning appropriate resources accordingly. Approved changes can be subsequently scheduled into target releases, in line with the policy for determining releases. The result is an updated Change Schedule, containing details of all approved changes and their implementation dates, along with the Projected Service Availability document, containing details of changes to agreed service level agreements and service availability.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[18]

- OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[19]
- UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[20]

These agreements can be in a draft or finalized status.

Inputs

- Change_ Assessed (From: A514)

  The change, including the collection of assessment recommendations.
- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).
- Asset Requisition Status (From: A552)

  The acknowledgement, including status information such as expected dates, that a requisition for one or more assets has been received and processed.
- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

Outputs

- Change Request_ Rejected

  Any change request which has been rejected, and sent back to the requestor. Reasons for rejection include:
  - Lack of authorization or funding
  - The change requested is beyond the scope of Change Management (for example, it is a new requirement)
  - The change request is incomplete or in error
  - The change request has been assessed as having too high a risk and needs rework
- Project Proposal (To: A3 A34 A342 A35 A352 A36 A364)

  A formal statement of an idea being put forward for consideration that includes the business case for the proposed IT investment.
- Projected Service Outage (To: A244 A734)

  As defined in ITIL: “A Document that identifies the effect of planned Changes, maintenance Activities and Test Plans on agreed Service Levels.” [21]
- Change Schedule (To: A514 A516 A517 A52 A522 A525 A54 A543 A545 A6 A63 A632 A66 A665 A7 A74 A744 A745 A75 A752 A753)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of

18. ITIL V3 Glossary
19. ITIL V3 Glossary
20. ITIL V3 Glossary
21. ITIL V3 Glossary

Change, even though it also contains information about Changes that have already been implemented." [22]

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change (To: A412 A516 A517 A518 A52 A522 A53 A532 A54 A543 A753)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

[A516] Coordinate Change Implementation

Description

This activity takes an approved change and coordinates its implementation. If the approved change involved creating or updating a solution, then the solution components must first be built and supplied by Solution Realization.

Approved changes are made available primarily through Release Management, but some changes are implemented through assignment by the Change Manager (within Change Management). This determination is made by Change Management policies and the appropriate change model.

Change Management monitors the actual deployment of the change, as carried out by Deployment Management.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

Inputs

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: "A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented."[23]

22. ITIL V3 Glossary
23. ITIL V3 Glossary

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Standard Change (From: A513)

  Those changes that have been pre-approved for deployment. They include well known and proven tasks, and have limited (and well understood) or no impact on the integrity of the target context, such as the infrastructure. These changes will also have all entitlement issues, like financial approvals, and licensing already resolved.

  Implementation can be either user-driven or managed by the IT function. Examples include:

  - Installation of printer drivers from a pre-installed library on a PC
  - Downloading and installation of software or fixes from vendor sites
  - Upgrading a laptop to a larger hard drive

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests. (From: A52 A524)Release Acceptance Request

  A request for final approval from Change Management for a release to be able to proceed to rollout. The request will be accompanied by evidence of the release having passed its acceptance criteria.

- Implementation Progress Data (From: A375 A52 A523 A524 A53 A535 A536 A635)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

Outputs

- Change Schedule (To: A514 A516 A517 A52 A522 A525 A54 A543 A545 A6 A63 A632 A66 A665 A7 A74 A744 A745 A75 A752 A753)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[24]

- Release Acceptance (To: A52 A524 A525)

  The notification of approval that the Release can proceed to its rollout activities.

- Change Implementation Communication (To: A375 A52 A522 A523 A524 A53 A535 A536 A54 A542 A543 A635 A655 A665)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

24. ITIL V3 Glossary

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships.

- Incident (To: A537 A6 A65 A652)

  A fault in IT service and infrastructure that has been reported, or an event that could cause an interruption to one or more services. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a service request and becomes an incident once it is determined that a fault is being reported.

- Asset Data Update Package (To: A553)

  All status and detail changes to an asset after the initial creation. Includes lease, license, maintenance changes and, at end of life, disposal notification. An additional example is a change in standard currency exchange rates from the IT Financial Management process.

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change_ Implemented (To: A517 A518)

  The history and record of the change implementation activity which has culminated in the completion of the change related to the change request. It also includes the case of a failed implementation, with any back out results.

[A517] Review and Close Change

Description

This activity contains the tasks involved in reviewing all implemented changes, after a predefined period has elapsed or another review trigger has been activated. It ensures that the change has had the desired effect and met its objectives, and that users and customers are content with the results, or to identify any shortcomings. The review activity determines whether the implementation plan and the back-out plan worked correctly, and whether the change was implemented on time and to cost. It determines whether any follow up action (such as the creation of a new change request) is required.

A formal close of the change is performed. The closure of a change includes updating other process areas of the status of the change.

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

Inputs

- Change_ Implemented (From: A516)

  The history and record of the change implementation activity which has culminated in the completion of the change related to the change request. It also includes the case of a failed implementation, with any back out results.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[25]

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

Outputs

- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Change_ Closed (To: A518)

  The change having completed all parts of the change life cycle, and reached *closed* status.

[A518] Monitor and Report Change Management

Description

This activity is responsible for looking over all changes, whether active or closed, and being able to provide information on the status and details of one or many changes. The other activities in Change Management each update change data maintained in *change records*, defined in ITIL as: “A Record containing the details of a Change. Each Change Record documents the Lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.”[26]

The information can be provided in an ad hoc manner or using predetermined reports. This scope is inclusive of the other parts of Change Management. In addition, it examines detailed information and summary statistics about the volumes, success rates, and issues with the workings of changes outside this process:

- The deployment activities coordinated by Change Management
- Standard changes (so those changes not requiring direct Change Management coordination)

25. ITIL V3 Glossary
26. ITIL V3 Glossary

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

Inputs

- Change_ Closed (From: A517)

  The change having completed all parts of the change life cycle, and reached *closed* status.
- Change_ Implemented (From: A516)

  The history and record of the change implementation activity which has culminated in the completion of the change related to the change request. It also includes the case of a failed implementation, with any back out results.
- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.
- Change_ Assessed (From: A514)

  The change, including the collection of assessment recommendations.
- Change_ Categorized (From: A513)

  The change request, which has completed acceptance, is now recognized as a change. The categorization indicates the types and levels of assessment needed.
- Change Request_ Recorded (From: A512)

  The details of a change request, captured in a document or other format defined by the Change Management Framework.
- Change Status and Information Request

  A request for the current status of a change within the control of Change Management.
- Deployment Reports (From: A538)

  Report about how well deployments are progressing or have been completed.
- Service Request Reports (From: A615)

  Any reports that reflect the status of service requests with the purpose to control the quality of service fulfillment, the compliance with existing SLAs, for planning purposes and as a basis for improvements.

Outputs

- Change Information (To: A2 A23 A233 A235 A3 A35 A355 A513 A514 A515 A516 A517 A54 A542 A543 A6 A61 A613 A615 A62 A621 A63 A632 A64 A641 A65 A654 A66 A662 A666 A7 A72 A721 A725 A73 A731 A735 A736 A74 A741 A742 A743 A75 A751 A76 A761 A764)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.
- Change Management Activity Data (To: A519)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A519] Evaluate Change Management Performance

Description

This activity describes the tasks required to assess the efficiency and effectiveness of the Change Management process. It includes the capture of information on change records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Change Management process remains fit for purpose and identifies where changes to the process might be required. Examples of topics addressed include:

- Assessing the Change Advisory Board (CAB) and its effectiveness
- Analyzing policies and procedures
- Analyzing rejected change requests
- Analyzing change failures
- Analyzing change successes

Controls

- Change Management Framework (From: A511)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Change Management process will operate to meet its mission and goals.

Inputs

- Change Management Activity Data (From: A512 A513 A514 A515 A516 A517 A518)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

Outputs

- Change Management Evaluation (To: A511)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

[A52] Release Management

Purpose

The purpose of the Release Management process is to prepare and finalize release packages that are fit for deployment so that optimal business value will be attained when deployment occurs.

Definition of release: “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.” [27]

Outcomes

As a result of the successful implementation of the Release Management process:

- Release packages – whether supporting new business capability, improvement in cost performance, or other advances in service quality - form the basis for deployment
- Deployment risks to existing service quality are minimized
- Customer and user satisfaction upon release deployment is increased
- All implications to the parties involved in deploying or receiving a release are identified and validated prior to the deployment event
- Only authorized releases are introduced into the live environment

Scope

Release Management spans the planning and direction of the rollout of software, hardware, and operational processes including related documentation, and operating procedures. The changes that comprise the release are managed by Change Management, and their inclusion in the release can be determined by time, technology interdependencies, target, risk mitigation, organization, scale (multiple copies) or service dependencies. The design of the release will need to consider how rollout is achieved. For example, whether or not the release can be requested by a user using a self-service selection and then installed automatically and transparently.

Includes

- Release design, creation, and testing
  - For example, implementation scripts
- Specifying the deployment model for a release. The deployment model provides a template of the activities and plans from which specific deployment instances can be customized for geography, scale, local conditions, and other factors
- Checking and testing training materials and incorporating them into the deployment model
- Verification of successful release package installation, including ensuring that the integrity of function has been maintained
- Roll back (also known as back out) mechanisms and procedures

Excludes

- Solution Realization (creation of functionality, usage procedures, training materials, and any other release deliverable) (Realization category)

27. ITIL V3 Glossary

- Testing of solution functionality (Solution Test)
- Management of change requests (Change Management)
- Deployment of release packages (Deployment Management)

Controls

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[28]

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[29]

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[30]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[31]

28. ITIL V3 Glossary
29. ITIL V3 Glossary
30. ITIL V3 Glossary
31. ITIL V3 Glossary

- UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[32]

These agreements can be in a draft or finalized status.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

Inputs

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Release Acceptance (From: A51 A516)

  The notification of approval that the release can proceed to its rollout activities.

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Product Package (From: A3 A35 A353 A354 A355)

  A description of the product that details how it is to be iteratively assembled, integrated and deployed, as well as the status of the product itself as it migrates through the various stages of realization, deployment and operation.

32. ITIL V3 Glossary

- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- Solution Plans and Commitments (From: A4 A41 A42 A422 A425 A43 A432 A44 A442 A45 A452)

  The collective overall information on both the development plan for the solution and the content of the solution as it progresses from concept to reality.

  - Plans: Sets of committed solution phases, activities, tasks and milestones together with timeframe.
  - Commitments: Sets of requirements, designs and other deliverables, such as test cases.

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Solution_ Accepted (From: A4 A45 A456)

  The Solution which has been approved by the stakeholder community, and is now ready to be deployed.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Service Resilience Plans (From: A7)

  The collection of plans produced by the individual processes involved in ensuring the resilience within service management. Processes contributing are:

  - Compliance Management
  - Security Management
  - Availability Management
  - Capacity Management
  - Facilities Management
  - IT Service Continuity Management (See the definition of the *plan* output from each individual process for more details.)

Outputs

- Solution Design Request (To: A42 A422)

  A formal communication that authorizes and triggers the Solution Analysis and Design process (usually beginning at the conceptual design level).

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- Release Strategy (To: A523 A524 A525 A526 A53 A532 A533 A534 A535 A536 A537 A538)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

- Release Notice (To: A53 A534 A535)

  The notices and other communications material, about a release, that is made available to both users and IT staff impacted by the release. Contents will range from general awareness announcements through specific details, such as training schedules and plans, to actual release documentation and training material. They are updated as experience is gained about the release.

- Release (To: A53 A532 A533 A535 A536)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[33]

- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Release Acceptance Request (To: A51 A516 A525)

  A request for final approval from Change Management for a release to be able to proceed to rollout. The request will be accompanied by evidence of the release having passed its acceptance criteria.

Activities

This process is composed of these activities:

- A521 Establish Release Management Framework
- A522 Plan Release Strategy
- A523 Design and Build Release
- A524 Test and Verify Release
- A525 Monitor and Report Release
- A526 Review and Close Release
- A527 Evaluate Release Management Performance

33. ITIL V3 Glossary

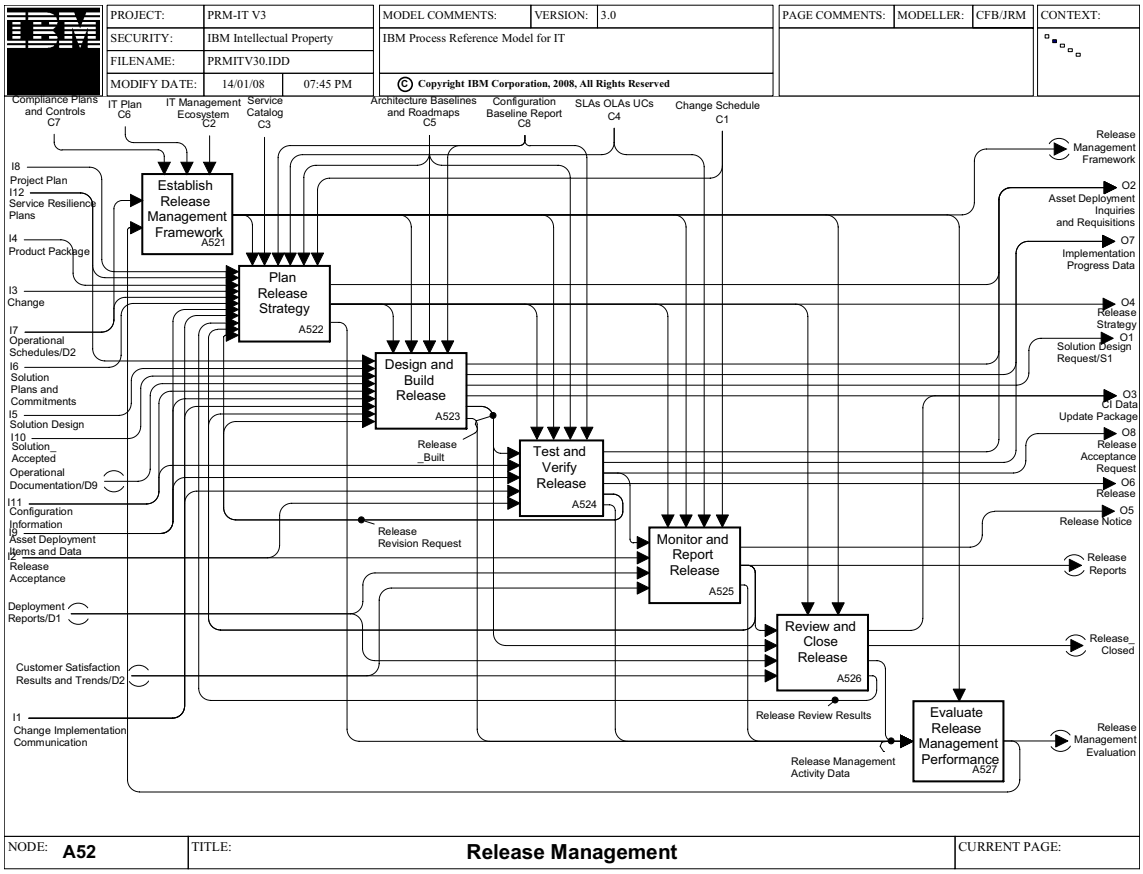

Figure 3. A52 Release Management

[A521] Establish Release Management Framework

Description

A framework and guidelines for Release Management are developed based on business and IT strategy. The tasks in this activity include:

- Understanding the requirements and specifications for Release Management practices
- Enacting the strategy for Release Management automated support
- Defining evaluation criteria for Release Management solutions and services
- Establishing the framework for Release Management by defining and implementing practices and systems that support process activities
- Determining skill requirements for the staff and assigning staff based on these systems

Finally, the structure and process of Release Management including escalation responsibilities have to be communicated to the process users.

The establishment of the process framework also includes the continuous improvement of Release Management, meaning the consideration of the Release Management process evaluation and the implementation of recommended improvement actions.

Controls

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

- The items for which compliance is required
- The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
- The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

It will be the major vehicle for communications and guidance on compliance efforts.

- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

Inputs

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Release Management Evaluation (From: A527)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

Outputs

- Release Management Framework (To: A522 A523 A524 A525 A526 A527)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.

[A522] Plan Release Strategy

Description

This activity determines the strategy for how each release is defined and then brought into existence in a state ready for deployment. It includes understanding the constituents of the release (from one or more Service Packages) and then considering the impact of the one or more authorized changes, which relate to the release contents in order to create the overall plan for the release. The planning covers building, testing and verifying the release (including the possible need for pilot deployments), as well as establishing a model for how the finalized release should be deployed.

Controls

- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[34]

- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer.

34. ITIL V3 Glossary

Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

ITIL definition of these terms:

- SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[35]
- OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[36]
- UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[37]

These agreements can be in a draft or finalized status.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[38]

Inputs

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

- Service Resilience Plans (From: A7)

  The collection of plans produced by the individual processes involved in ensuring the resilience within service management. Processes contributing are:

  - Compliance Management
  - Security Management
  - Availability Management
  - Capacity Management
  - Facilities Management
  - IT Service Continuity Management

  (See the definition of the *plan* output from each individual process for more details.)

- Product Package (From: A3 A35 A353 A354 A355)

  A description of the product that details how it is to be iteratively assembled, integrated and deployed, as well as the status of the product itself as it migrates through the various stages of realization, deployment and operation.

35. ITIL V3 Glossary
36. ITIL V3 Glossary
37. ITIL V3 Glossary
38. ITIL V3 Glossary

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Solution Plans and Commitments (From: A4 A41 A42 A422 A425 A43 A432 A44 A442 A45 A452)

  The collective overall information on both the development plan for the solution and the content of the solution as it progresses from concept to reality.

  - Plans: Sets of committed solution phases, activities, tasks and milestones together with timeframe.
  - Commitments: Sets of requirements, designs and other deliverables, such as test cases.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Release Review Results (From: A526)

  Analysis of release usage, with identification of successes and areas for release improvement.

- Release Reports (From: A525)

  Reports showing the outcome of the release implementations.

- Release Revision Request (From: A524)

  Identification of a need to re-plan a release following the outcomes of test and acceptance work.

Outputs

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Release Strategy (To: A523 A524 A525 A526 A53 A532 A533 A534 A535 A536 A537 A538)

  The overall approach which will guide the release through its complete lifecycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

- Release Management Activity Data (To: A527)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A523] Design and Build Release

Description

This activity determines what needs to be built for the release and how it will be assembled and deployed. During this activity, the release build, installation, and rollback scripts are designed at a high level. In addition, software and hardware components are obtained for the build activity and the test environment is put in place.

After the release has been designed, this activity builds the scripts and other aspects needed to assemble and to deploy the release. This includes

- Creating the build environment
- Creating build, install, and rollback scripts
- Placing software in the DML
- Creating support, training, and deployment documentation
- Updating the CMS with information about the release package

Controls

- Release Strategy (From: A52 A522)

  The overall approach which will guide the release through its complete lifecycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.
- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

Inputs

- Service Resilience Plans (From: A7)

  The collection of plans produced by the individual processes involved in ensuring the resilience within service management. Processes contributing are:

  - Compliance Management
  - Security Management
  - Availability Management

- Capacity Management
- Facilities Management
- IT Service Continuity Management

(See the definition of the *plan* output from each individual process for more details.)

- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- Solution_ Accepted (From: A4 A45 A456)

  The Solution which has been approved by the stakeholder community, and is now ready to be deployed.

- Operational Documentation (From: A855)

  The subset of *knowledge assets* that represent the set of material, both externally provided and internally generated, required to support the development, deployment, operation, and maintenance of solutions and services.

  - ITIL uses the term Operational Document Library to refer to an implementation of this output.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Release Reports (From: A525)

  Reports showing the outcome of the release implementations.

- Release Revision Request (From: A524)

  Identification of a need to re-plan a release following the outcomes of test and acceptance work.

Outputs

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Solution Design Request (To: A42 A422)

  A formal communication that authorizes and triggers the Solution Analysis and Design process (usually beginning at the conceptual design level).

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
- Release _BuiltRelationships. (To: A524 A526)

  The release ready for testing.
- Release Management Activity Data (To: A527)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A524] Test and Verify Release

Description

This activity takes the built release package and tests to determine if installation, configuration, and rollback work properly. If successful, the release is ready for deployment. If not, the release must go through another round of either design or build, and a subsequent retesting.

After testing, the release package is either accepted or rejected.

Controls

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.
- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Configuration Baseline Report (From: A54 A542 A543)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

Inputs

- Release _Built (From: A523)

  The release ready for testing.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Release Acceptance (From: A51 A516)

  The notification of approval that the release can proceed to its rollout activities.

Outputs

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Release Acceptance Request (To: A51 A516 A525)

  A request for final approval from Change Management for a release to be able to proceed to rollout. The request will be accompanied by evidence of the release having passed its acceptance criteria.

- Release (To: A53 A532 A533 A535 A536)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[39]

- Release Revision Request (To: A522 A523)

  Identification of a need to re-plan a release following the outcomes of test and acceptance work.

- Release Management Activity Data (To: A527)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

39. ITIL V3 Glossary

[A525] Monitor and Report Release

Description

This activity monitors the progress of the release as it might be updated and throughout its deployment instances, and produces the required reporting. The reports provide both users and IT staff with the communications material such as general awareness, training schedules and plans, actual release documentation, and training content.

Controls

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[40]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[41]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The

40. ITIL V3 Glossary
41. ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[42]

These agreements can be in a draft or finalized status.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: "A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented."[43]

Inputs

- Release Acceptance Request (From: A52 A524)

  A request for final approval from Change Management for a release to be able to proceed to rollout. The request will be accompanied by evidence of the release having passed its acceptance criteria.

- Release Acceptance (From: A51 A516)

  The notification of approval that the release can proceed to its rollout activities.

- Deployment Reports (From: A538)

  Report about how well deployments are progressing or have been completed.

- Customer Satisfaction Results and Trends (From: A27 A276)

  A report summarizing current customer satisfaction results and historical data. Can be used to identify trends.

Outputs

- Release Notice (To: A53 A534 A535)

  The notices and other communications material, about a release, that is made available to both users and IT staff impacted by the release. Contents will range from general awareness announcements through specific details, such as training schedules and plans, to actual release documentation and training material. They are updated as experience is gained about the release.

- Release Reports (To: A522 A523 A526)

  Reports showing the outcome of the release implementations.

- Release Management Activity Data (To: A527)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

42. ITIL V3 Glossary
43. ITIL V3 Glossary

[A526] Review and Close Release

Description

This activity examines the information relating to the usage of a release in order to identify what has worked well and what has not. For the latter, it works to identify improvements in any aspect of the release. These aspects can include:

- Success rates from deploying the release
- Efficiency, in both people and technical resource, in deploying the release
- User feedback on missing and erroneous documentation and usage guidance

This activity includes checking the actual performance and outcomes of the new or changed service against the requirements.

When the Release Strategy indicates that a particular release is to be *closed* (in other words, no longer be available for deployment), this activity will perform the tasks associated with achieving that objective.

Controls

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.
- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.

Inputs

- Release Reports (From: A525)

  Reports showing the outcome of the release implementations.
- Release _Built (From: A523)

  The release ready for testing.
- Deployment Reports (From: A538)

  Report about how well deployments are progressing or have been completed.
- Customer Satisfaction Results and Trends (From: A27 A276)

  A report summarizing current customer satisfaction results and historical data. Can be used to identify trends.

Outputs

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships
- Release_ Closed

  Information and technical content related to the closure of a release.
- Release Management Activity Data (To: A527)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.
- Release Review Results (To: A522)

  Analysis of release usage, with identification of successes and areas for release improvement.

[A527] Evaluate Release Management Performance

Description

This activity looks at the performance of the Release Management process and identifies improvement opportunities for the Release Management Framework. This includes examining:

- Adequacy of release management resources
- Rejected or failed releases
- Trends in the effectiveness and efficiency in managing releases
- Release Management policies and procedures

Controls

- Release Management Framework (From: A521)

  This framework describes:

  - Types of releases
  - Naming and other release conventions
  - Release policies and procedures
  - Definitive Media Library (DML) specifications
  - Roles and responsibilities
  - Scheduling policies
  - Process review schedule.

  This framework provides governance information for the other activities in Release Management.

Inputs

- Release Management Activity Data (From: A522 A523 A524 A525 A526)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

Outputs

- Release Management Evaluation (To: A521)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

[A53] Deployment Management

Purpose

The purpose of the Deployment Management process is to place releases and other desired changes into their target environments, and to activate them in order that the functionality and operational improvements they contain can create their intended value.

Definition of Deployment: “movement of new or changed hardware, software, documentation, Process, etc to the Live Environment.”[44]

The *other desired changes* includes transferring the responsibility for any subset of an IT endeavor’s operations from ownership by one service provider to another, while maintaining service continuity. For certain such transfers, deployment involves managing the effective transfer of resources necessary to deliver the service. Resources include staff, technology infrastructure, and intellectual capital.

Outcomes

As a result of the successful implementation of the Deployment Management process:

- New capability is introduced on a timely basis, and with minimized risk, disruption and cost
- Transfers of service responsibility are effected on a timely basis, and with minimized risk, disruption and cost
- All parties involved in a deployment (for example, users of the capabilities being deployed, service providers performing the deployment) are appropriately prepared, trained and skilled to ensure successful deployment
- In the event of failures during deployment, contingency plans ensure the expected level of service quality is delivered

Scope

Deployment Management is primarily triggered by an instruction to roll out any approved combination of software, related hardware, documentation, and operating procedures to one or more defined targets (for example: systems, user groups) within constraints such as cost and time. An alternative trigger for the instantiation of Deployment Management relates to the transfer of the responsibility for one or more services between providers or across business or organizational boundaries. At the other end of the scale, the implementation work related to a change which impacts a single CI is also performed by this process.

The completion of each deployment is indicated when the stakeholders affirm that the expected outcomes of a deployment are achieved and a business-as-usual operational service state has been attained.

Includes

- Deployment planning and co-ordination with affected parties
- Identification of resources (hardware, software, processes and procedures, and staff) to be deployed, or to be transferred between service providers
- Creating capabilities and procedures to support deployment activities, and to verify the readiness of and account for resources impacted
- Creating a plan for continuity of service

44. ITIL V3 Glossary

- Execution of the deployment plan, including:
  - Electronic distribution of software and other soft-copy items
  - Invoking logistical movements for physical items
  - Installing technical resources
  - Activating the desired configuration
  - Testing the installation against defined criteria (as provided in the Release Package and Change)
  - Back out of installed items, when needed
  - Delivering training
  - Providing initial user assistance
- Assessment of readiness to begin service delivery, and for handover to business-as-usual
- Management of risks and issues related to the deployment activities.

Excludes

- Logistics and movement of physical assets (Asset Management)
- Preparation and commissioning of the supporting environment (Facilities Management)
- Accounting for capital transfers and deployment expenditures (Financial Management)
- Program and project management techniques (Program and Project Management)
- Achievement of business benefits from new functionality (IT Customer Transformation Management)
- Updates to the CMS (Configuration Management)
- Knowledge and skill transfer (Knowledge Management)

Controls

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.
- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.
- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.
- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as

operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

ITIL definition of these terms:

- SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[45]
- OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[46]
- UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[47]

These agreements can be in a draft or finalized status.

- IT Budget (From: A8 A81 A813)

  The planned IT funding broken down in relevant ways, such as activities and milestones per period, to reflect the contents of the IT plan.

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

Inputs

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[48]

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions

45. ITIL V3 Glossary
46. ITIL V3 Glossary
47. ITIL V3 Glossary
48. ITIL V3 Glossary

- Instructions for the next stages of implementation

This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Release Notice (From: A52 A525)

  The notices and other communications material, about a release, that is made available to both users and IT staff impacted by the release. Contents will range from general awareness announcements through specific details, such as training schedules and plans, to actual release documentation and training material. They are updated as experience is gained about the release.

- Release (From: A52 A524)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as "A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity."[49]

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Service Resilience Plans (From: A7)

  The collection of plans produced by the individual processes involved in ensuring the resilience within service management. Processes contributing are:

  - Compliance Management
  - Security Management
  - Availability Management
  - Capacity Management
  - Facilities Management
  - IT Service Continuity Management

  (See the definition of the *plan* output from each individual process for more details.)

- Solution_ Accepted (From: A4 A45 A456)

  The Solution which has been approved by the stakeholder community, and is now ready to be deployed.

- Service Request_ Authorized (From: A6 A61 A613)

  The communication of a service request which has completed screening and is being passed to one or more other processes for actual fulfillment. It includes control information from the screening (assessment) such as priority assigned and committed completion target.

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

49. ITIL V3 Glossary

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

Outputs

- Solution_ Deployed (To: A3 A32 A4 A43 A433 A44 A443 A6 A62 A63 A634 A64 A641 A7 A76)

  The new or adjusted solution in *live* status, ready for useful work within its target environment, and reflecting the outcome of the deployment activities.

  The deployed solution includes documentation, procedures, training materials, support guidance as well as the primary solution contents.

- Incident (To: A537 A6 A65 A652)

  A fault in IT service and infrastructure that has been reported, or an event that could cause an interruption to one or more services. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a service request and becomes an incident once it is determined that a fault is being reported.

- Solution Design Request (To: A42 A422)

  A formal communication that authorizes and triggers the Solution Analysis and Design process (usually beginning at the conceptual design level).

- Customer Satisfaction Issue (To: A27 A274)

  Any determination of a customer satisfaction issue. Can be either direct form a customer, or prompted by any IT staff member in carrying out other processes.

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships.

- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.

Activities

This process is composed of these activities:

- A531 Establish Deployment Management Framework
- A532 Plan Deployment Program
- A533 Prepare Deployment Capabilities
- A534 Perform Transition Administration
- A535 Perform Deployment
- A536 Verify Deployment and Activate Service
- A537 Review and Close Deployment
- A538 Monitor and Report Deployment Program
- A539 Evaluate Deployment Management Performance

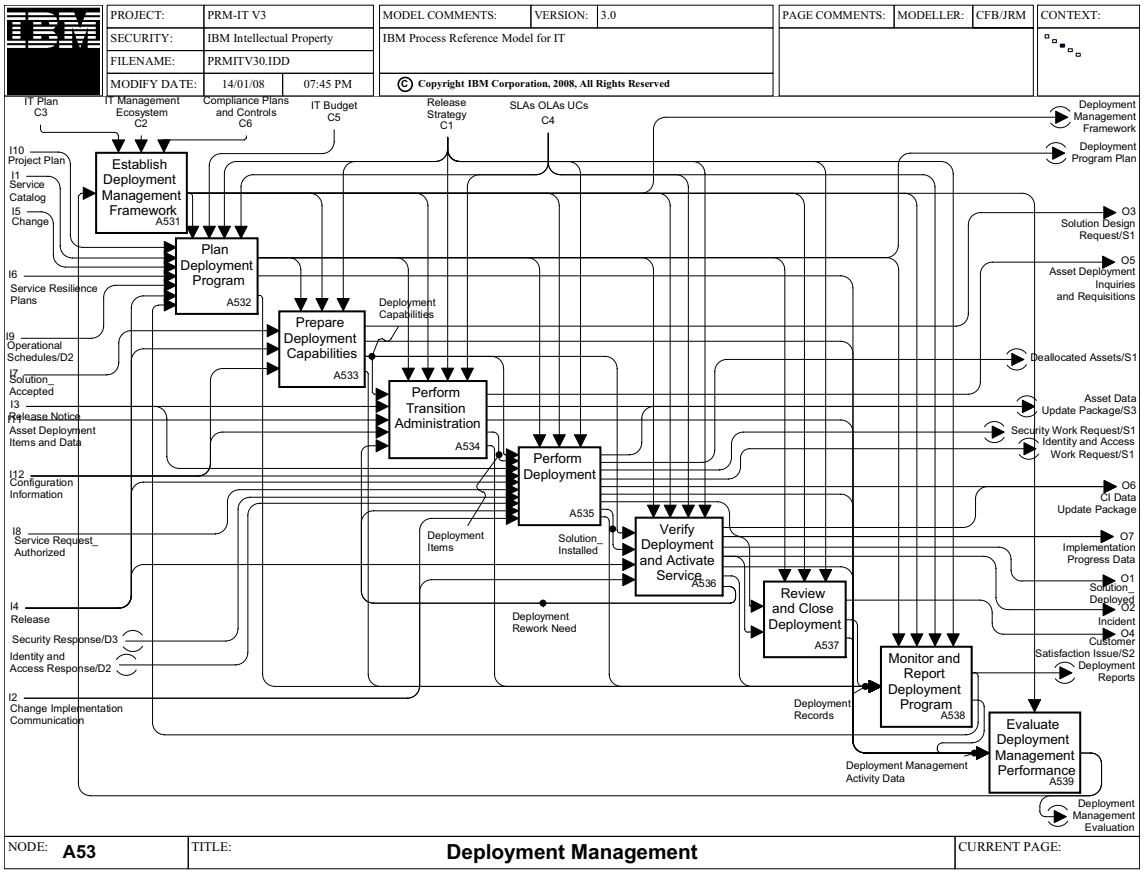

Figure 4. A53 Deployment Management

[A531] Establish Deployment Management Framework

Description

This activity involves creating or updating the Deployment Management Framework. It addresses:

- Policies and procedures
- Roles and responsibilities
- Technical standards
- Deployment models
- Process measurements and controls
- Process review schedule.

This framework provides governance information for the other activities in Deployment Management.

Controls

- IT Plan (From: A3 A36 A365)

  The set of approved projects and associated schedule, operating plan, service level management commitments, and resource allocation commitments and adjustments for a defined fiscal or planning cycle.

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.
- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

Inputs

- Deployment Management Evaluation (From: A539)

  An analysis of deployment management activity data providing an understanding of the current success or failure of the deployment management process, and an identification of potential process improvements.

Outputs

- Deployment Management Framework (To: A532 A533 A534 A535 A536 A537 A538 A539)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

[A532] Plan Deployment Program

Description

In this activity, the deployment plan details are generated concerning specifically what will be done during deployment. This includes:

- Assignment of individuals to specific activities
- Detailed sequence of events
- Specifications of requirements (number, type) for assets to be ordered and delivered as part of each deployment event
- Identification of the CIs installed, changed, and removed
- Multi-site plans
- Restoration plans
- Plans for communicating the deployment to stakeholders
- Generating release notes for users

Deployment plan details will vary depending upon the type of deployment. Deployment types include:

- Rollouts involving site preparation, siting and installation of physical machinery, and other activities requiring on-site availability of deployment personnel
- Software distribution, both

- *Pushed* from a deployment control point
- *Pulled* for example, by a user invoking a download and install

- Education and training events in support of technology introduction
- Transfer of responsibility between providers (with or without any alteration in service content or quality)

Controls

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- IT Budget (From: A8 A81 A813)

  The planned IT funding broken down in relevant ways, such as activities and milestones per period, to reflect the contents of the IT plan.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[50]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[51]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[52]

  These agreements can be in a draft or finalized status.

50. ITIL V3 Glossary
51. ITIL V3 Glossary
52. ITIL V3 Glossary

Inputs

- Project Plan (From: A3 A37 A374)

  The set of work plans. Work plans can include management, human resource, technical environment, project quality, communications management, among others.

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[53]

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Service Resilience Plans (From: A7)

  The collection of plans produced by the individual processes involved in ensuring the resilience within service management. Processes contributing are:

  - Compliance Management
  - Security Management
  - Availability Management
  - Capacity Management
  - Facilities Management
  - IT Service Continuity Management

  (See the definition of the *plan* output from each individual process for more details.)

- Operational Schedules (From: A621)

  The overall schedule for individual work items and when they are processed. Examples are start and stop times of specific applications, availability of specific services and infrastructure services (file transfer).

- Release (From: A52 A524)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[54]

- Deployment Reports (From: A538)

  Report about how well deployments are progressing or have been completed.

53. ITIL V3 Glossary
54. ITIL V3 Glossary

Outputs

- Deployment Program Plan (To: A533 A534 A535 A536 A537 A538)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process, to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.
- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.
- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.

[A533] Prepare Deployment Capabilities

Description

This activity prepares the Deployment Capabilities required for a given deployment. Examples include:

- Training staff to be able to execute deployment tasks
- Creating a facility for volume pre-installation of base software prior to delivery to the ultimate destination
- Customizing standard release or solution materials to target site needs

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.
- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

Inputs

- Solution_ Accepted (From: A4 A45 A456)

  The Solution which has been approved by the stakeholder community, and is now ready to be deployed.
- Release (From: A52 A524)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[55]
- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

Outputs

- Solution Design Request (To: A42 A422)

  A formal communication that authorizes and triggers the Solution Analysis and Design process (usually beginning at the conceptual design level).
- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.
- Deployment Capabilities (To: A534 A535 A536)

  Combination of knowledge, skills, experience, processes, systems and technologies required to deploy new or changed deployment objects into the target environment.
- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.

[A534] Perform Transition Administration

Description

In this activity, the administrative and other tasks of a preparatory nature for the transition to the desired deployment status are performed. The tasks include:

- Requisitioning hardware and software assets for deployment
- Making logistical arrangements
- Executing transfers of ownership

55. ITIL V3 Glossary

The activity ensures that appropriate data on assets is provided to the Asset Management process to reflect their updated status. Items impacted include location, financial status (support contracts), and ownership.

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[56]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[57]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The

56. ITIL V3 Glossary
57. ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[58]

These agreements can be in a draft or finalized status.

Inputs

- Deployment Capabilities (From: A533)

  Combination of knowledge, skills, experience, processes, systems and technologies required to deploy new or changed deployment objects into the target environment.

- Release Notice (From: A52 A525)

  The notices and other communications material, about a release, that is made available to both users and IT staff impacted by the release. Contents will range from general awareness announcements through specific details, such as training schedules and plans, to actual release documentation and training material. They are updated as experience is gained about the release.

- Asset Deployment Items and Data (From: A5 A55)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Deployment Rework Need (From: A536)

  The identification that any parts of the deployment plan need to be reworked prior to the capability reaching full service status. Everyday changes in business operations within the organization that is the target of deployment can be the cause of such a need. For example, changes in staff since plan creation.

Outputs

- Asset Deployment Inquiries and Requisitions (To: A55)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.

- Asset Data Update Package (To: A553)

  All status and detail changes to an asset after the initial creation. Includes lease, license, maintenance changes and, at end of life, disposal notification. An additional example is a change in standard currency exchange rates from the IT Financial Management process.

- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Deployment Items (To: A535)

  The collection of items that are ready for deployment and for which all title and ownership information reflects the imminent deployment into the target environment. These items are instances of what ITIL calls Service Assets, defined as "Any Capability or Resource of a Service Provider."[59]

- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.

58. ITIL V3 Glossary
59. ITIL V3 Glossary

[A535] Perform Deployment

Description

This activity performs the physical, technical, and other tasks (such as delivering training and registering users) which move the capabilities being deployed from *not deployed* to *deployed*. It includes:

- Distribution and installation of hardware and software, ensuring appropriate data is provided for asset and configuration updates
- Customization, where needed, of:
  - CIs to reflect their specific usage context
  - Identity and access records (by initiating updates using the Identity and Access Management process)
  - Security mechanisms (also using update requests, to the Security Management process)
- Removal of redundant services and assets, (processes, procedures and tools).
- Introduction of new or changed processes to the service provider teams responsible for Service Management activities.

Perform deployment has fulfilled its responsibilities when the capability being deployed is ready for verification and activation.

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.
- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.
- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

Inputs

- Deployment Capabilities (From: A533)

  Combination of knowledge, skills, experience, processes, systems and technologies required to deploy new or changed deployment objects into the target environment.

- Deployment Items (From: A534)

  The collection of items that are ready for deployment and for which all title and ownership information reflects the imminent deployment into the target environment. These items are instances of what ITIL calls Service Assets, defined as “Any Capability or Resource of a Service Provider.”[60]

- Release Notice (From: A52 A525)

  The notices and other communications material, about a release, that is made available to both users and IT staff impacted by the release. Contents will range from general awareness announcements through specific details, such as training schedules and plans, to actual release documentation and training material. They are updated as experience is gained about the release.

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Release (From: A52 A524)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[61]

- Service Request_ Authorized (From: A6 A61 A613)

  The communication of a service request which has completed screening and is being passed to one or more other processes for actual fulfillment. It includes control information from the screening (assessment) such as priority assigned and committed completion target.

- Security Response (From: A726)

  The result of processing a security request. The result will reflect a range of possibilities, depending on the nature of the service request:

  - For a protection request the protections put in place
  - For an access authorization request the success or failure of the request

- Identity and Access Response (From: A673 A674)

  The result of processing an identity and access request. The result will reflect a range of possibilities, depending on the nature of the request:

  - For an identity request actions taken to create, maintain, or delete the identity
  - For an access (rights) request the success or failure of the request, with relevant information describing the status of access rights

- Deployment Rework Need (From: A536)

  The identification that any parts of the deployment plan need to be reworked prior to the capability reaching full service status. Everyday changes in business operations within the organization that is the target of deployment can be the cause of such a need. For example, changes in staff since plan creation.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions

60. ITIL V3 Glossary
61. ITIL V3 Glossary

- Instructions for the next stages of implement

This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

Outputs

- Asset Data Update Package (To: A553)

  All status and detail changes to an asset after the initial creation. Includes lease, license, maintenance changes and, at end of life, disposal notification. An additional example is a change in standard currency exchange rates from the IT Financial Management process.

- Deallocated Assets (To: A552)

  Assets that are no longer deployed to specific owners. These assets are free to be allocated to new owners.

- Security Work Request (To: A72)

  A Security Request originating from another process.

- Identity and Access Work Request (To: A67)

  An identity and access request originating from another process.

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Solution Installed (To: A536)

  A solution under deployment for which all tasks required to achieve deployment status have been completed other than final activation.

- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.

[A536] Verify Deployment and Activate Service

Description

This activity verifies the integrity of the solution under deployment and transitions the new changed service to Service Operations.

Integrity testing can include the following items:

- Service assets and capabilities are in place
- Documentation updates are completed
- Learning material has been made available to stakeholders
- Users are prepared to operate the new or changed service
- Measurements and reporting systems are established.

Transition to full service status can include a defined period as *early life support*; defined by ITIL as "Support provided for a new or Changed IT Service for a period of time after it is Released. During Early Life Support the IT Service Provider may review the KPIs, Service Levels and Monitoring Thresholds, and provide additional Resources for Incident and Problem Management."[62]

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

62. ITIL V3 Glossary

- SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[63]
- OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[64]
- UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[65]

These agreements can be in a draft or finalized status.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

Inputs

- Deployment Capabilities (From: A533)

  Combination of knowledge, skills, experience, processes, systems and technologies required to deploy new or changed deployment objects into the target environment.

- Solution Installed (From: A535)

  A solution under deployment for which all tasks required to achieve deployment status have been completed other than final activation.

- Release (From: A52 A524)

  The packaging of one or more solutions along with all the materials (scripts, documentation, for example) needed for successful deployment.

  In ITIL, Release is defined as “A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.”[66]

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implement

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

Outputs

- CI Data Update Package (To: A5 A54 A542 A543)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

63. ITIL V3 Glossary
64. ITIL V3 Glossary
65. ITIL V3 Glossary
66. ITIL V3 Glossary

  - Attributes
  - Relationships.
- Implementation Progress Data (To: A51 A516 A537)

  The record of each incremental activity performed as part of the implementation of a change or release.
- Solution_ Deployed (To: A3 A32 A4 A43 A433 A44 A443 A6 A62 A63 A634 A64 A641 A7 A76)

  The new or adjusted solution in live status, ready for useful work within its target environment, and reflecting the outcome of the deployment activities.

  The deployed solution includes documentation, procedures, training materials, support guidance as well as the primary solution contents.
- Incident (To: A537 A6 A65 A652)

  A fault in IT service and infrastructure that has been reported, or an event that could cause an interruption to one or more services. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a service request and becomes an incident once it is determined that a fault is being reported.
- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.
- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.
- Deployment Rework Need (To: A534 A535)

  The identification that any parts of the deployment plan need to be reworked prior to the capability reaching full service status. Everyday changes in business operations within the organization that is the target of deployment can be the cause of such a need. For example, changes in staff since plan creation.

[A537] Review and Close Deployment

Description

This activity reviews the tasks completed during deployments and determines that all objectives of the deployment plan were met. A management plan is established for outstanding risks, issues, incidents and known errors before the deployment is closed. Deployment is completed with a handover of the support to Service Operations.

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

Inputs

- Implementation Progress Data (From: A375 A52 A523 A524 A53 A535 A536 A635)

  The record of each incremental activity performed as part of the implementation of a change or release.

- Incident (From: A2 A27 A273 A5 A51 A516 A53 A536 A61 A613 A62 A625 A63 A637 A64 A644 A646 A67 A675 A7 A72 A75 A754)

  A fault in IT service and infrastructure that has been reported, or an event that could cause an interruption to one or more services. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a service request and becomes an incident once it is determined that a fault is being reported.

Outputs

- Customer Satisfaction Issue (To: A27 A274)

  Any determination of a customer satisfaction issue. Can be either direct form a customer, or prompted by any IT staff member in carrying out other processes.

- Deployment Records (To: A538)

  A set of records containing the details of each deployment program and each deployment instance within that program.

- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A538] Monitor and Report Deployment Program

Description

This activity ensures that the overall set of deployment programs and all of the deployment instances within each program are monitored throughout their entire life cycles.

Aspects include:

- Maintaining currency and integrity of data on deployments
- Monitoring status and deployment impact on service level agreements
- Identification of any requirement for deployment instance: *reprioritization* or *escalation*
- Communicating status and progress to stakeholders and support groups

Controls

- Deployment Program Plan (From: A532)

  The set of plans for achieving the deployment of an identified set of information technology capabilities. Items covered include:

  - Specification of coordinated deployment tasks and procedures to move new or changed hardware, software, documentation, process to the target environment
  - Rollout timetables for deployments that are repeated, and associated logistical plans
  - Identifying personnel resources necessary to achieve each deployment event, and obtaining commitments for their availability

  The deployment program will cover aspects such as locations, target systems, dates, persons affected (both users and IT service provider staff), required communications, and training plan.

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

- SLAs, OLAs, UCs (From: A2 A24 A243)

  The agreements that represent the interlinked set of commitments for the service utility and warranty that is to be provided to one or more customers. The agreement between the customer and the organizational unit that directly provides the service is known as a service level agreement (SLA) and is visible to the customer. The agreements that represent the commitments of the collective set of internal organizational units and external entities to provide identified sub-components of the overall service are known as operational level agreements (OLAs). OLAs are not usually visible to the customer. Contractual statements of the commitments by external entities are known as underpinning contracts (UCs).

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[67]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[68]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[69]

  These agreements can be in a draft or finalized status.

- Release Strategy (From: A52 A522)

  The overall approach that will guide the release through its complete life cycle, and into deployment. It includes the plan for creating a release, including the definition of the set of changes which are collected within it, and also the release test plan.

67. ITIL V3 Glossary
68. ITIL V3 Glossary
69. ITIL V3 Glossary

Inputs

- Deployment Records (From: A532 A533 A534 A535 A536 A537)

  A set of records containing the details of each deployment program and each deployment instance within that program.

Outputs

- Deployment Reports (To: A518 A525 A526 A532)

  Report about how well deployments are progressing or have been completed.
- Deployment Management Activity Data (To: A539)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A539] Evaluate Deployment Management Performance

Description

This activity looks at the performance of the Deployment Management process and determines if changes to the Deployment Management Framework should be recommended. This includes examining:

- Adequacy of release management resources
- Rejected or failed deployments
- Deployment Management policies and procedures

Controls

- Deployment Management Framework (From: A531)

  This framework describes the policies, procedures, organizational roles and responsibilities, and other information under which the Deployment Management process will operate to meet its mission and goals.

  This framework provides governance information for the other activities in Deployment Management.

Inputs

- Deployment Management Activity Data (From: A532 A533 A534 A535 A536 A537 A538)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

Outputs

- Deployment Management Evaluation (To: A531)

  An analysis of deployment management activity data providing an understanding of the current success or failure of the deployment management process, and an identification of potential process improvements.

[A54] Configuration Management

Purpose

The purpose of the Configuration Management process is to maintain the integrity of the configuration items (CIs) employed in, or related to, IT systems and infrastructure in either a development or operational context, and to provide accurate information about CIs and their relationships.

Configuration Management emerged out of complementary needs within both IT development and IT operations. IT development needs to maintain the integrity of evolving development artifacts in a development project. Similarly, IT operations should maintain the integrity of CIs that have been made operational.

Definition of a configuration item: “Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.”[70]

Outcomes

As a result of the successful implementation of this process:

- All configuration items within IT systems and infrastructure are accurately identified and cataloged
- All configuration items are adequately tracked and controlled
- Authorized requests to obtain CIs from secure libraries or stores (or to return them) are satisfied promptly and accurately
- Accurate configuration information is provided in response to informational requests
- Any exceptions between configuration records and the corresponding CIs are identified and corrected
- In development projects: development CIs in multiple development streams are controlled and coordinated

Scope

Relationship with Asset Management

To properly understand Configuration Management, it is necessary to understand its relationship with Asset Management. Asset Management keeps track of things of value (assets) to an IT organization, whether that value is financial, technical, or otherwise, throughout the asset's entire life cycle. That life cycle stretches from the time the asset is ordered or commissioned to the time when it is retired and disposed.

At various stages in an asset's life cycle, the usage of that asset can cause it to become a part of some larger object requiring management (for example, a processor is added to a pool of processors allocated to a particular task) or it can be split into a number of parts at smaller granularity (for example, a physical server is operated as several virtual servers). Similarly, an ERP system licensed from a vendor might represent one or a handful of assets to be tracked (for financial or contract management purposes), whereas it can represent hundreds of modules which

70. ITIL V3 Glossary

must be identified individually. For example, for local customization, problem determination, or maintenance patch application purposes.

The characteristic of these events is that the asset has been applied to some defined purpose, typically through any or all of the Solution Development and Integration process, the Release Management process and the Deployment Management process. At these times, those parts become configuration items (CIs) and are managed by Configuration Management. Configuration Management focuses on the internal and external relationships of a CI and addresses the configuration needs of a stage in an asset's life cycle.

For instance, during development of a software asset, Configuration Management might be used for source code control of the components that make up that asset. Another instance is when a system becomes operational within the IT infrastructure. In that instance, Configuration Management is used to maintain operational information about that CI and its relationships to other CIs in the IT infrastructure. The two most widely recognized uses of Configuration Management are *development* Configuration Management and *operations* Configuration Management.

Configuration Management in Development and Operations

Configuration Management addresses the needs of both IT development and IT operations. The characteristics of these domains are similar,[71] yet also have differences. Similarities include:

- Both development and operations focus on the various configuration items that make up their domains. In development, these include evolving hardware, software, and documentation that constitute an IT system being developed. In operations, these include fully developed hardware, software, and documentation that have been deployed and made operational within the IT infrastructure.
- Both development and operations maintain information about CIs and their relationships.
- On a regular basis, that information is checked for accuracy against the actual configuration items and inaccurate information is corrected.

Differences between *development* Configuration Management and *operations* Configuration Management include:

- IT development maintains the integrity of development CIs primarily by controlling the CIs themselves, whereas IT operations maintains the integrity of operational CIs by controlling information about the CIs.
- Check-in/check-out of IT development CIs is a normal practice in Configuration Management for IT development. (There is a distinct difference in how check-in and check-out is performed for electronic as opposed to physical CIs.) IT operations does not perform check-in/check-out of CIs.
- IT operations focuses on controlling updates to information about CIs. Significant information about CIs must be manually maintained. In contrast, information about development CIs is primarily obtained from the CI itself.
- Development CIs (such as software and hardware components and document chapters) are typically smaller-grained than operational CIs (such as PCs, applications, servers, and others).
- The configuration management system for IT development (often called a source code control system) is typically maintained separately from the configuration management system for IT operations, and the technology and procedures used by each system is usually different.
- The CIs that make up an operational IT infrastructure are typically also considered assets. However, most CIs in a development project are not considered to be assets because their value to the IT organization is considered too small (or too intangible) to track. For this

71. Industry examples of this can be seen in ISO/IEC 15288 Systems and Software Engineering - System Life Cycle Processes and ISO/IEC 12207 Systems and Software Engineering - Software Life Cycle Processes.

reason, a development project might have few *assets* tracked by Asset Management other than the overall system under development.

The similarities in Configuration Management between IT development and IT operations are sufficient to define a single process at a high level. The differences between IT development and IT operations are significant only at a lower level of the process.

Common Data

In practical terms, Asset Management and Configuration Management carry out their activities using data about these assets and CIs, which is largely common to them both, though each has some attributes and relationships not significant to the other. Successful implementation of both processes requires joint work on their data models and clear rules (that is, governance) on which process *owns* any shared attribute.

Types of CIs

The ITIL definitions of asset and of configuration item include a range of types of IT elements which can fall under Configuration Management. Whether an implementation covers all or just some of these types, it is likely that there will be some process aspects that are dependent on the needs of different component types. Consideration of a few examples illustrates this:

- Each hardware item is a candidate for both configuration and asset management, though probably at different levels of granularity. An IT organization will want to keep track of that hardware item throughout its life cycle from the standpoint of Asset Management. At the same time, when that system is operational, Configuration Management might be interested in internal hardware components (which are CIs) as well as other CIs that have some operational relationship to this CI. Hardware items cannot usually be cloned.
- Software components might have no record in the asset register. They can be subject to tight access controls (for example, to avoid erroneous multiple update during development) and at the same time they can be cloned to create as many instances as needed within limitations such as license counts. Larger software elements, such as applications can be both a CI as well as an asset.

The process will also need to take into account the arrangement of the set of internal and external service providers and establish appropriate interfaces with the Configuration Management process of those service providers.

Includes

- Establishing naming conventions for configuration items and relationships
- Designing, creating, populating, and updating the Configuration Management System (CMS)
- Managing movements into and out of secure libraries
- Supporting configuration item audits
- Identifying configuration item interdependencies
- Linking configuration item changes to specific change requests (RFCs)
- Defining and reporting configuration baselines

Excludes

- Inventory tracking (Asset Management)
- Procurement of configuration items (Supplier Management)
- Tuning and installing configuration items (Capacity Management, Deployment Management)
- Assets that are not CIs, such as:

  - Items ordered but not received
  - Items no longer in operation
  - Bulk inventory
  - Assets not operationally managed

Controls

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[72]

- Service Catalog (From: A2 A23 A235)

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.

  ITIL defines Service Catalog as: “A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.”[73]

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

Inputs

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions

72. ITIL V3 Glossary
73. ITIL V3 Glossary

- Instructions for the next stages of implementation

This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- CI Data Update Package (From: A4 A42 A424 A43 A433 A434 A435 A436 A437 A44 A444 A45 A456 A51 A516 A52 A523 A526 A53 A535 A536 A6 A63 A634 A64 A645 A65 A652 A7 A75 A753 A754)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- CI Requisition (From: A4 A42 A423 A424 A43 A433 A434 A44 A444)

  A request for one or more CIs to be made available so that they can be worked upon. In a development environment, this might be a request to check-out solution components from a version-controlled configuration library.

- Configuration Information Request (From: A336 A422 A423 A424 A442 A443 A664)

  Any request for information about one or more configuration items. Many IT processes will make such requests.

- Asset Information (From: A5 A55 A553)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.

Outputs

- CIs (To: A4 A43 A434 A44 A444)

  CIs are the technical (in its broadest sense) components, including assemblies of more granular components, upon which IT service is based. The relevant extract from the ITIL definition of Configuration Item is: “Any Component that needs to be managed in order to deliver an IT Service. ... CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs."[74]

- Configuration Baseline Report (To: A423 A51 A514 A516 A52 A522 A523 A524)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

- Configuration Information (To: A3 A33 A336 A4 A42 A422 A423 A424 A44 A442 A443 A51 A513 A514 A516 A52 A523 A524 A53 A533 A534 A535 A545 A55 A553 A6 A61 A612 A62

74. ITIL V3 Glossary

A623 A63 A634 A635 A64 A642 A65 A652 A653 A654 A66 A662 A67 A674 A7 A72 A724 A726 A727 A73 A735 A736 A74 A742 A743 A744 A75 A752 A76 A764 A765 A766)

The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Change Request (To: A5 A51 A512)

  Change requests (also known as RFCs) are the means for submitting proposed change and actual change activity in the environment. Change requests can be triggered for a wide variety of reasons, from a broad spectrum of sources. They can be concerned with any part of the environment or with any service or activity.

Activities

This process is composed of these activities:

- A541 Establish Configuration Management Framework
- A542 Identify Configuration Items
- A543 Control Configuration Items
- A544 Report Configuration Status
- A545 Verify and Audit Configuration Items
- A546 Evaluate Configuration Management Performance

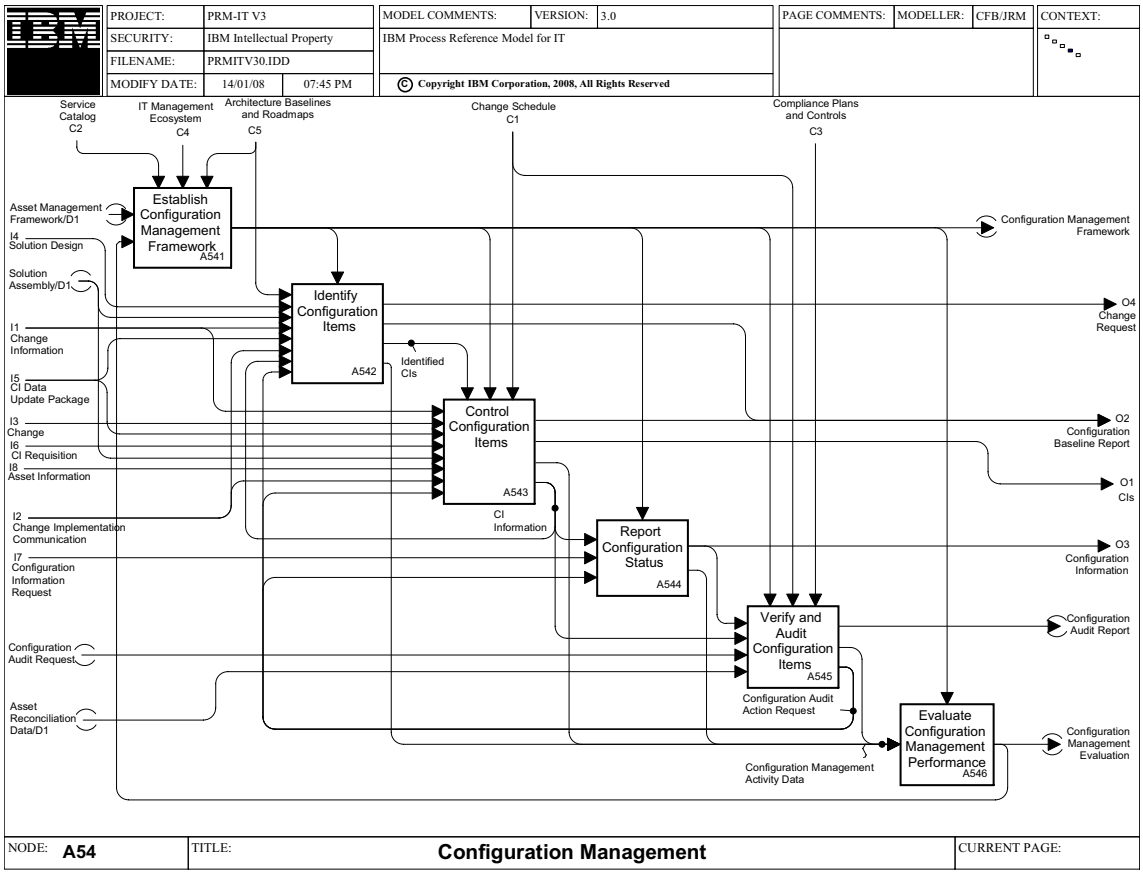

Figure 5. A54 Configuration Management

[A541] Establish Configuration Management Framework

Description

The framework for Configuration Management should be consistent with business and IT models and strategies, as well as general IT guidelines and practices.

The tasks in this activity include:

- Understanding the requirements of the overall IT Management System for Configuration Management
- Defining the strategy, policies, and conventions for controlling configuration items, including:
  - Creation of configuration baselines
  - License control
  - Version numbering and control
  - Identification of approved procedures that may make changes to the CMS
  - Identification of procedures related to workspaces, branching, and merging
  - Generic naming conventions
  - Generic configuration item status codes
  - Attributes necessary for all CI types
  - CI control procedures, such as check-in/check-out procedures
  - Generic information and integration standards for all CMDBs within the CMS

It should be noted that specific practices for individual CI types are defined in Identify Configuration Items.

- Designing, championing, and overseeing the implementation of Configuration Management solutions
- Defining ownership and relationships within the Configuration Management System (CMS). Within an operations context, the CMS represents all CIs within the IT infrastructure. Within a development context, the CMS represents all artifacts used to create the system under development.
- Identifying roles and responsibilities, determining skill requirements for the staff and assigning staff
- Defining process metrics and practices for collecting those metrics
- Establishing two-way agreements with other parties where there is a mutual requirement for configuration information and control.

Finally, the structure and process for Configuration Management (including procedures and tools) must be communicated to the process users and stakeholders.

The establishment of the Configuration Management Framework also includes the continuous improvement of Configuration Management. For example, the consideration of the Configuration Management process evaluation and the implementation of recommended improvement actions.

Controls

- Service Catalog

  Catalog of all services offered for delivery by the IT service provider. Portions of it can be used as a means of communication to the customers, but there are also sections that describe details (usually not published outside the delivery organization) of how each service is provided.(From: A2 A23 A235)

  ITIL defines Service Catalog as: "A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes."[75]

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

Inputs

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.

- Configuration Management Evaluation (From: A546)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

Outputs

- Configuration Management Framework (To: A542 A543 A544 A545 A546 A551)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

[A542] Identify Configuration Items

Description

This activity defines the types of configuration items under the control of Configuration Management. This might be done during the initial population of a CMDB within the Configuration Management System (CMS) or when a new type of CI is identified for inclusion within the CMS. This discovery can be done manually or automatically.

As a result of design at either the architectural level or within a particular solution, a new CI type can be generated that should be reflected within the CMS schema.

Once a new type of CI is identified, a number of steps might need to occur, including:

- Creating specific naming conventions for this CI type
- Creating specific labeling conventions

75. ITIL V3 Glossary

- Defining attributes for the CI type
- Defining documentation for the CI type
- Defining relationships to other CI types
- Defining specific control procedures

This information is stored in the Configuration Identification Practices.

Each of the decisions can result in an update to or modification of the CMS schema, resulting in a proposal to update the CMS.

Controls

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

Inputs

- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.

- Solution Assembly (From: A43)

  The collection of all the work products created during solution development and integration, including prototypes or implementation of parts of a solution for evaluation and analysis purposes.

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

- CI Data Update Package (From: A4 A42 A424 A43 A433 A434 A435 A436 A437 A44 A444 A45 A456 A51 A516 A52 A523 A526 A53 A535 A536 A6 A63 A634 A64 A645 A65 A652 A7 A75 A753 A754)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions
  - Instructions for the next stages of implementation

  This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- CI Information (From: A543)

  The definitive configuration information about each and every managed configuration item. The collection of this information is represented by the concept of a CMDB.

- Configuration Audit Action Request (From: A545)

  A request for some corrective action to be taken to reflect the outcomes of configuration audit.

Outputs

- Change Request (To: A5 A51 A512)

  Change requests (also known as RFCs) are the means for submitting proposed change and actual change activity in the environment. Change requests can be triggered for a wide variety of reasons, from a broad spectrum of sources. They can be concerned with any part of the environment or with any service or activity.

- Configuration Baseline Report (To: A423 A51 A514 A516 A52 A522 A523 A524)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

- Identified CIs (To: A543)

  The set of CI types, with details of their:

  - Attributes
  - Relationships
  - Structures in which they are expected to participate

- Configuration Management Activity Data (To: A546)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A543] Control Configuration Items

Description

All transactions with the CMS are carefully controlled so that only authorized access is allowed. The functionality of a CMS can vary based on the context in which it works. For example, in an operations context, the CMS stores information about CIs within the IT infrastructure and transactions with the CMS will include creating new CI records, deleting CI records, and updating existing CI records. In a counter example, within a software development context, the CMS stores an electronic version of the CI itself and transactions with the CMS will include creating or deleting CIs within the build structure as well as checking in and checking out CIs for development work. Regardless of the context, all transactions (whether additions, deletions, cloning or branching, merging, or modifications) are recorded in the CMS.

As noted previously, CI transactions can include information about CIs or could be electronic versions of the CIs themselves (if the CIs are software modules in a development environment). Submitted CI transactions are validated, and then checked for proper authorization. Specific operational procedures might already be approved for specific types of transactions with the CMS. (For example, service desk personnel might have authority to update records within an operations CMS, or developers within a software development project might have such authority within a development CMS.) Non-typical requests can be routed to a person to obtain proper authorization or rejected outright, based upon policy.

During processing of the transaction, relevant linkages to other CIs and to any other information, such as change requests, will also be defined, checked and recorded.

New configuration baselines can be generated based on configuration management practices. A baseline might be created within an operations context to help restore a set of CIs to a known stable state if a change or release fails. In a development context, a baseline represents a known state of a system under development to which the project could return if necessary.

Controls

- Identified CIs (From: A542)

  The set of CI types, with details of their:

  - Attributes
  - Relationships
  - Structures in which they are expected to participate

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[76]

Inputs

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.

- Change (From: A51 A515)

  A change, triggered by a change request, which has successfully completed assessment and has subsequently been authorized for implementation. The authorization includes details of schedule options and any implementation conditions, such as the decision to include the change within the scope of a planned release.

- CI Data Update Package (From: A4 A42 A424 A43 A433 A434 A435 A436 A437 A44 A444 A45 A456 A51 A516 A52 A523 A526 A53 A535 A536 A6 A63 A634 A64 A645 A65 A652 A7 A75 A753 A754)

  The details of modifications to any existing CIs that must be validated and captured in the CI master data. The modifications can include:

  - Attributes
  - Relationships

- CI Requisition (From: A4 A42 A423 A424 A43 A433 A434 A44 A444)

  A request for one or more CIs to be made available so that they can be worked upon. In a development environment, this might be a request to check-out solution components from a version-controlled configuration library.

- Solution Assembly (From: A43)

  The collection of all the work products created during solution development and integration, including prototypes or implementation of parts of a solution for evaluation and analysis purposes.

- Asset Information (From: A5 A55 A553)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.

- Change Implementation Communication (From: A51 A516)

  Information used to coordinate and implement a change. It can reflect either or both the:

  - Status of the overall change as a result of carrying out previous instructions

76. ITIL V3 Glossary

- Instructions for the next stages of implementation

This dual nature is required to reflect incremental progress towards completion of a multi-stage implementation, especially when the outcome of one or more steps did not meet expectations in all respects.

- Configuration Audit Action Request (From: A545)

  A request for some corrective action to be taken to reflect the outcomes of configuration audit.

Outputs

- Configuration Baseline Report (To: A423 A51 A514 A516 A52 A522 A523 A524)

  A point-in-time snapshot of a portion of a CMDB that is relevant to one or more purposes from other IT management processes. This can include past, current, and future projected instances.

- CIs (To: A4 A43 A434 A44 A444)

  CIs are the technical (in its broadest sense) components, including assemblies of more granular components, upon which IT service is based. The relevant extract from the ITIL definition of Configuration Item is: “Any Component that needs to be managed in order to deliver an IT Service. ... CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.” [77]

- Configuration Management Activity Data (To: A546)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- CI Information (To: A542 A544 A545)

  The definitive configuration information about each and every managed configuration item. The collection of this information is represented by the concept of a CMDB.

[A544] Report Configuration Status

Description

This activity makes CI and CMS information available to any authorized requestor. The information can range from detailed attributes and relationships to summarized information. It can cover an individual CI or a collection of CIs. It can be essentially unformatted raw data or predetermined reports. Finally, it can be provided in line with a planned schedule or in response to an individual request.

Controls

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

Inputs

- CI Information (From: A543)

  The definitive configuration information about each and every managed configuration item. The collection of this information is represented by the concept of a CMDB.

77. ITIL V3 Glossary

- Configuration Information Request (From: A336 A422 A423 A424 A442 A443 A664)

  Any request for information about one or more configuration items. Many IT processes will make such requests.

- Configuration Audit Action Request (From: A545)

  A request for some corrective action to be taken to reflect the outcomes of configuration audit.

Outputs

- Configuration Information (To: A3 A33 A336 A4 A42 A422 A423 A424 A44 A442 A443 A51 A513 A514 A516 A52 A523 A524 A53 A533 A534 A535 A545 A55 A553 A6 A61 A612 A62 A623 A63 A634 A635 A64 A642 A65 A652 A653 A654 A66 A662 A67 A674 A7 A72 A724 A726 A727 A73 A735 A736 A74 A742 A743 A744 A75 A752 A76 A764 A765 A766)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Configuration Management Activity Data (To: A546)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

[A545] Verify and Audit Configuration Items

Description

This activity determines how well the contents of the CMS match an audit target, such as a development baseline or the IT infrastructure. This configuration audit checks to make sure the CI information matches the physical reconciliation data, that naming conventions are followed, that the DML and DHS agree with the CI, and that change requests match the composition of the CI. The audit takes place on a regular basis, as stipulated by the Configuration Management Plan, or as requested by the Configuration Manager or other authorized personnel. Audits can help verify the effects of approved changes and can help identify unauthorized changes.

There are two contexts in which a configuration audit might take place. In both instances, the audit determines whether the contents of the CMS match some known collection of CIs. The first context is an operations context, and the purpose of the audit is to determine if the contents of the CMS matches the existing CIs in the IT infrastructure. The second context is a development context, and the purpose of the audit is to determine if the development baseline contains all development CIs in the CMS. The audit takes place on a regular basis, as stipulated by the Configuration Management Plan, or as requested by the Configuration Manager or other authorized personnel.

Controls

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

- Change Schedule (From: A5 A51 A515 A516)

  As defined in ITIL: “A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.”[78]

78. ITIL V3 Glossary

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

Inputs

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- CI Information (From: A543)

  The definitive configuration information about each and every managed configuration item. The collection of this information is represented by the concept of a CMDB.

- Configuration Audit Request (From: A554 A716)

  A request for any aspect of the collected configuration information to be audited against the actual, real managed object.

- Asset Reconciliation Data (From: A554)

  Data collected during auditing and inspection of assets. Typically includes location, condition and verification results.

Outputs

- Configuration Audit Report (To: A455 A554 A716)

  The outcomes of a configuration audit. The outcomes cover both status of configuration items and audit trails of changes to configuration items, such as logs of identities of the people making such changes.

- Configuration Management Activity Data (To: A546)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

- Configuration Audit Action Request (To: A542 A543 A544)

  A request for some corrective action to be taken to reflect the outcomes of configuration audit.

[A546] Evaluate Configuration Management Performance

Description

This activity analyzes the Configuration Management process and its effectiveness. This includes:

- Identifying suggested improvements to the Configuration Management Plan
- Analyzing CI requests to determine how to improve the processing of such requests
- Analyzing CI information errors to determine how to improve the quality of information received
- Analyzing stakeholder needs

All of this analysis is used to create a Configuration Management Performance Evaluation. This will be a key input when updating the Configuration Management Framework.

Controls

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.

Inputs

- Configuration Management Activity Data (From: A542 A543 A544 A545)

  Data resulting from all work carried out by each process activity. Examples would be volumes, timings, resources used, success and error rates, interfaces invoked, rework, customer feedback, priorities.

Outputs

- Configuration Management Evaluation (To: A541)

  An assessment of the overall performance of the process against the targets set in the process framework and an identification of possible process improvement areas.

[A55] Asset Management

Purpose

The purpose of the Asset Management process is to control all assets owned by the IT endeavor throughout their life cycle and to maintain accurate information about them in an Asset Register. The aspects of asset control under this purpose include inventory, contractual (licensing, maintenance), ownership and location

ITIL provides the following definitions:

- Asset: “Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organisation, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.”[79]
- Asset Register: “A list of Assets, which includes their ownership and value. The Asset Register is maintained by Asset Management.”[80]

The definition of *asset* is much broader than those in widespread usage within the IT industry.[81] In this model, many of the types identified are controlled by other processes specialized for the management issues that pertain to them.

- Items Management, Organization, Process are the subject of the IT Governance and Management System category of processes
- Knowledge Management is a process in its own right
- People are recruited, developed, and assigned to responsibilities by the Workforce Management process
- Financial Capital is under the custodianship of the Financial Management process, with interfaces to this process where Asset activities have an impact on financial valuation (for example, by a decision to dispose of an asset or to transfer ownership to a new owner).

The technology object types Information, Applications, Infrastructure are all covered by this process, where each individual item can qualify for any of the asset control purposes in scope. For example, it is not unusual for accessories for PCs (such as keyboards, mice) to be excluded from asset control.

Outcomes

As a result of the successful implementation of the Asset Management process:

- Value is maximized from technology assets over their lifetime
- Assets are provided in an accurate and timely manner to supply, movement or other requests
- Accurate and timely information about technology assets supports informed IT decision making, at both strategic and tactical levels
- Exposure to risks relating to IT assets is minimized
- IT assets are managed in compliance with legal, industry and corporate standards and requirements
- Governance of assets drives the right trade-offs in investments in asset and usage of assets

79. ITIL V3 Glossary
80. ITIL V3 Glossary
81. See HTTP://en.wikipedia.org/wiki/IT_asset_management

Scope

Asset Management has dual responsibilities:

1. To control each asset from initial creation (such as receipt from suppliers) through all life cycle events (such as change of location, transfer of ownership, change of use) until eventual retirement or disposal.
2. To identify, collect, maintain, control, and report inventory and financial information about IT assets throughout their life cycle

Includes

- License management (including software license compliance)
- Lease and maintenance administration of each asset
- Inventory management (includes physical components and specifications)
- Allocation of available assets to meet approved requests
- Physical logistics (such as transportation) of assets
- Retirement of outdated assets
- Triggering requisition for the procurement of additional assets (for example, if a policy of maintaining minimum inventory stock levels for standard, frequently needed asset item is in place)
- Financial life cycle of assets (including valuation)

Excludes

- Risk Management
- Contract and Supplier Management (including Procurement) (Supplier Management)
- Configuration Management (logical relationships)
- Managing the security of an asset (Facilities Management, Security Management)

Controls

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.
- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.

- IT Budget (From: A8 A81 A813)

  The planned IT funding broken down in relevant ways, such as activities and milestones per period, to reflect the contents of the IT plan.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)

Inputs

- Asset Deployment Inquiries and Requisitions (From: A433 A434 A51 A514 A515 A516 A52 A522 A523 A524 A53 A534)

  Requests for information about assets needed as part of deploying solutions, requisitions for allocation of assets, and notifications to trigger the delivery or distribution of these resources.
- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.
- Service Request_ Authorized (From: A6 A61 A613)

  The communication of a service request which has completed screening and is being passed to one or more other processes for actual fulfillment. It includes control information from the screening (assessment) such as priority assigned and committed completion target.
- Underpinning Contracts (From: A8 A82 A823)

  Content of contracts with suppliers, including terms and conditions, service level agreements (SLAs), among others. Covers both the actual contract itself, and information about it that is available as input for supplier evaluation and to other internal processes, such as financial management.

  Information Technology Infrastructure Library (ITIL) defines underpinning contract as “a contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in an SLA.”[82]
- IT Financial Reports (From: A8 A81 A813 A814 A815)

  All reports on financial data of IT for different stakeholders. Covers a wide range of reports from outlining projected costs through after-the-fact financial analyses.

Outputs

- Asset Deployment Items and Data (To: A4 A43 A51 A52 A522 A523 A524 A53 A534)

  Information about specific asset availability and requisition status, and also the actual asset items being offered up for deployment.
- Asset Information (To: A54 A543 A7 A71 A713 A72 A724 A8 A81 A812 A814 A815)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.

82. ITIL V3 Glossary

Activities

This process is composed of these activities:

- A551 Establish Asset Management Framework
- A552 Ready and Control Asset
- A553 Control Asset Information
- A554 Monitor, Audit and Reconcile Asset Records
- A555 Oversee Asset Contracts and Financials
- A556 Retire and Dispose of Asset
- A557 Report Asset Information
- A558 Evaluate Asset Management Performance

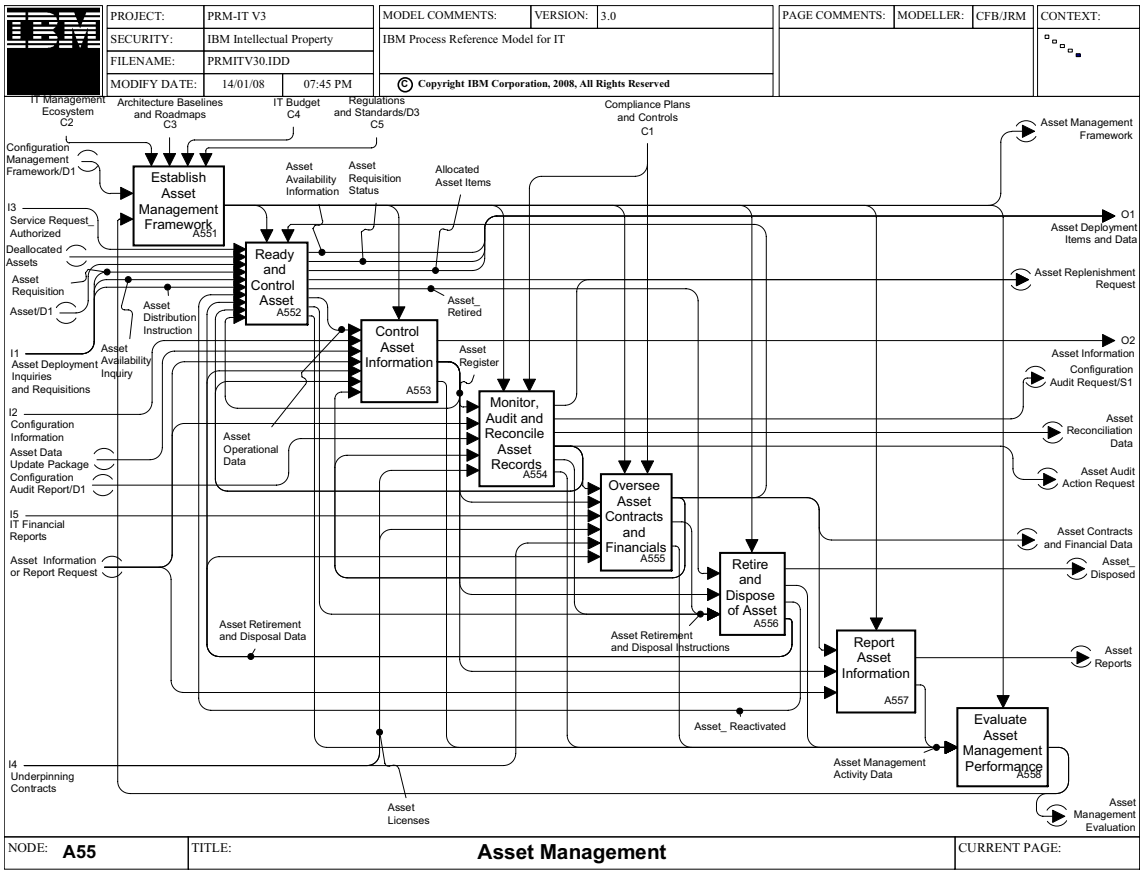

Figure 6. A55 Asset Management

[A551] Establish Asset Management Framework

Description

Define and maintain a framework of policies and procedures that guides and governs the behavior of the Asset Management process and its activities.

Incorporate mandatory elements from the IT Management Ecosystem.

Define a set of metrics to be used by each process for measuring and reporting performance.

Review process evaluations based on analysis of current performance, and approve recommendations for improvements. Refine the metrics to encourage process vitality and cost effectiveness.

Incorporate updated metrics and process change recommendations into the framework and communicate the changes.

Controls

- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- IT Budget (From: A8 A81 A813)

  The planned IT funding broken down in relevant ways, such as activities and milestones per period, to reflect the contents of the IT plan.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)

Inputs

- Configuration Management Framework (From: A541)

  The information and artifacts which represent the purposes of the process and the means by which the process will operate to satisfy them.
- Asset Management Evaluation (From: A558)

  Assessment results for the Asset Management process and its activities, including process performance metrics and the identification of potential process improvement items.

Outputs

- Asset Management Framework (To: A541 A552 A553 A554 A555 A556 A557 A558 A751)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.

[A552] Ready and Control Asset

Description

Prepare assets that are to be made available to users. This includes receiving the asset either from an asset provider or from the recycling of existing assets.

Prior to deployment, respond to inquiries concerning the status of the asset (such as whether it has been shipped from the vendor or not). Prepare assets for deployment (such as installing IT approved images, appropriate asset ID tags, among others). Allocate assets to specific users or sites, based on distribution instructions, and transfer assets to their appropriate locations.

Determine when to retire an asset.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.
- Asset Contracts and Financial Data (From: A555)

  Business records about an asset and related financial information. This includes data such as asset records, vendor information, asset costs and current value, tax data.

Inputs

- Service Request_ Authorized (From: A6 A61 A613)

  The communication of a service request which has completed screening and is being passed to one or more other processes for actual fulfillment. It includes control information from the screening (assessment) such as priority assigned and committed completion target.
- Deallocated Assets (From: A535)

  Assets that are no longer deployed to specific owners. These assets are free to be allocated to new owners.
- Asset (From: A82 A824)

  Each asset that has completed the procurement process (business now holds the title) and is available for productive deployment. During its useful life, it is managed by the Asset Management process.
- Asset Requisition

  The placement of an *order* for one or more specified assets (or asset types) to be *delivered* or otherwise made available for productive use.
- Asset Availability Inquiry

  A planning inquiry to establish the outlook for the availability of specified IT assets for productive use.

- Asset Distribution Instruction

  The formal trigger for IT assets, probably already reserved for this purpose, to be distributed. The instruction would include details such as:

  - Date
  - Location
  - Quantity
  - Specification
  - Personnel involved and contact details.
- Asset_ Reactivated (From: A556)

  An asset that was previously retired, but has been brought back into active service.
- Asset Retirement and Disposal Data (From: A556)

  Data that describes the disposition and status of assets slated for retirement and disposal.
- Asset Audit Action Request (From: A554)

  A request to perform some action based on the findings of an asset audit. This can include instructions such as to locate a known asset or to reassign it.
- Asset Register (From: A553)

  The complete set of records in asset information repositories.

Outputs

- Asset Availability Information (To: A514)

  Details of the ability of the subject IT asset or assets to be made available for deployment or development use. The details will include:

  - Quantities
  - Specifications
  - Dates
  - Locations
- Asset Requisition Status (To: A515)

  The acknowledgement, including status information such as expected dates, that a requisition for one or more assets has been received and processed.
- Allocated Asset Items (To: A433 A434 A435 A436)

  The assignment and delivery (if appropriate) of identified IT assets to fulfill asset requisitions.
- Asset Replenishment Request (To: A824)

  A trigger to indicate that additional quantities of an asset are required in order to meet existing or anticipated requisitions.
- Asset_ Retired (To: A556)

  An asset that is to be removed from service. Such an asset will be in a storage location (such as the Definitive Hardware Store or DHS) until it is either restored (recovered) for active use or disposed.
- Asset Operational Data (To: A553)

  Relevant individual data values describing the specifics of the current state of an asset. Examples include:

  - Location
  - Owner
  - Maintenance contract end date
  - Original purchase price

- Asset Retirement and Disposal Instructions (To: A556)

  Directives concerning assets slated for retirement and disposal.

- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

[A553] Control Asset Information

Description

Maintain asset data model and create, update, or delete asset information based on update data provided by various sources. These sources include other processes that provide administration and support of assets and configuration items (such as Incident Management, Problem Management, and Configuration Management).

Manage the repository or set of repositories containing asset information. Carry out actions that reconcile issues with asset records. Asset information includes assets within the entire asset life cycle, including received assets, active assets, retired assets, and disposed assets.

Make available information about specific assets.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Asset Management process will operate to meet its mission and goals.

Inputs

- Asset Operational Data (From: A552)

  Relevant individual data values describing the specifics of the current state of an asset. Examples include:

  - Location
  - Owner
  - Maintenance contract end date
  - Original purchase price

- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.

- Asset Data Update Package (From: A516 A534 A535 A652 A753 A754)

  All status and detail changes to an asset after the initial creation. Includes lease, license, maintenance changes and, at end of life, disposal notification. An additional example is a change in standard currency exchange rates from the IT Financial Management process.

- Asset Information or Report Request

  A request to obtain information about a deployed asset. This request specifies whether the information should be in a formal report or simply provided asset data. It covers a range of request types, such as:

  - Need for information on an individual asset
  - A scheduled report
  - A request for an asset analysis report.

- Asset Retirement and Disposal Data (From: A556)

  Data that describes the disposition and status of assets slated for retirement and disposal.

- Asset Audit Action Request (From: A554)

  A request to perform some action based on the findings of an asset audit. This can include instructions such as to locate a known asset or to reassign it.

- Asset Contracts and Financial Data (From: A555)

  Business records about an asset and related financial information. This includes data such as asset records, vendor information, asset costs and current value, tax data.

Outputs

- Asset Information (To: A54 A543 A7 A71 A713 A72 A724 A8 A81 A812 A814 A815)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.

- Asset Register (To: A552 A554 A555 A556 A557)

  The complete set of records in asset information repositories.

- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

[A554] Monitor, Audit and Reconcile Asset Records

Description

Monitor IT assets to determine their overall health or status. Areas of interest include meeting licensing requirements, whether assets are sufficiently up to date, and compliance with security requirements, among others.

In addition, more formal auditing is performed to ensure that data in asset information repositories corresponds to assets in the physical environment. Audits match discovered inventory information with existing assets. Reconcile discrepancies between information repositories and the physical environment by either updating data in the information repositories or requesting changes to the physical environment. Also, the findings of an audit might result in a request for an audit of the IT configuration.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Asset Management process will operate to meet its mission and goals.

- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

Inputs

- Asset Register (From: A553)

- Asset Information or Report RequestThe complete set of records in asset information repositories.

  A request to obtain information about a deployed asset. This request specifies whether the information should be in a formal report or simply provided asset data. It covers a range of request types, such as:

  - Need for information on an individual asset
  - A scheduled report
  - A request for an asset analysis report.
- Configuration Audit Report (From: A545)

  The outcomes of a configuration audit. The outcomes cover both status of configuration items and audit trails of changes to configuration items, such as logs of identities of the person(s) making such changes.
- Asset Contracts and Financial Data (From: A555)

  Business records about an asset and related financial information. This includes data such as asset records, vendor information, asset costs and current value, tax data.
- Asset Licenses

  A documented permission to use an asset or set of assets. The license can contain specific terms and conditions, including details such as the number of users, any rights to copy and distribute, and the license period.

Outputs

- Asset Replenishment Request (To: A824)

  A trigger to indicate that additional quantities of an asset are required in order to meet existing or anticipated requisitions.
- Configuration Audit Request (To: A545)

  A request for any aspect of the collected configuration information to be audited against the actual, real managed object.
- Asset Reconciliation Data (To: A545)

  Data collected during auditing and inspection of assets. Typically includes location, condition and verification results.
- Asset Audit Action Request (To: A552 A553 A555)

  A request to perform some action based on the findings of an asset audit. This can include instructions such as to locate a known asset or to reassign it.
- Asset Retirement and Disposal Instructions (To: A556)

  Directives concerning assets slated for retirement and disposal.
- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

[A555] Oversee Asset Contracts and Financials

Description

Manage and control all asset contracts and related records. This includes lease agreements, leasing schedules, tax data, and financial data. Manage financial aspects of assets, including asset costs, current value, depreciation, and tax determination. Conduct negotiations concerning terms and warranties. Correlate underpinning contracts to asset records (including lease agreements and schedules, tax data, and financial information). Provide financial information concerning the need to retire assets.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities, and other information under which the Asset Management process will operate to meet its mission and goals.
- Compliance Plans and Controls (From: A7 A71 A714)

  The authoritative and comprehensive statement of:

  - The items for which compliance is required
  - The means (policies, data specifications, procedures, techniques, tools) to achieve compliance
  - The definition of required compliance metrics and reports by which conformance will be able to be demonstrated for required scrutiny

  It will be the major vehicle for communications and guidance on compliance efforts.

Inputs

- Asset Audit Action Request (From: A554)

  A request to perform some action based on the findings of an asset audit. This can include instructions such as to locate a known asset or to reassign it.
- Asset Register (From: A553)

  The complete set of records in asset information repositories.
- IT Financial Reports (From: A8 A81 A813 A814 A815)

  All reports on financial data of IT for different stakeholders. Covers a wide range of reports from outlining projected costs through after-the-fact financial analyses.
- Asset Licenses

  A documented permission to use an asset or set of assets. The license may contain specific terms and conditions, including details such as the number of users, any rights to copy and distribute, and the license period.
- Underpinning Contracts (From: A8 A82 A823)

  Content of contracts with suppliers, including terms and conditions, service level agreements (SLAs), among others. Covers both the actual contract itself, and information about it that is available as input for supplier evaluation and to other internal processes, such as financial management.

  Information Technology Infrastructure Library (ITIL) defines underpinning contract as “a contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in an SLA.”[83]

83. ITIL V3 Glossary

- Asset Retirement and Disposal Data (From: A556)

  Data that describes the disposition and status of assets slated for retirement and disposal.

Outputs

- Asset Contracts and Financial Data (To: A552 A553 A554 A557 A814 A825)

  Business records about an asset and related financial information. This includes data such as asset records, vendor information, asset costs and current value, tax data.
- Asset Retirement and Disposal Instructions (To: A556)

  Directives concerning assets slated for retirement and disposal.
- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

[A556] Retire and Dispose of Asset

Description

Collect assets scheduled for retirement and disposal. Return assets to storage (such as the Definitive Hardware Store or DHS). Some retired assets will be restored to active use, while others will be disposed of.

Prepare assets for disposal by removing data and harvesting any useful or recyclable components. Recycle designated assets by making them available for reuse (see Ready and Control Asset). Once properly prepared, transfer assets to be disposed to a disposal site for final processing.

Notify the asset status of all assets being retired or disposed.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.

Inputs

- Asset_ Retired (From: A552)

  An asset that is to be removed from service. Such an asset will be in a storage location (such as the Definitive Hardware Store or DHS) until it is either restored (recovered) for active use or disposed.
- Asset Register (From: A553)

  The complete set of records in asset information repositories.
- Asset Retirement and Disposal Instructions (From: A552 A554 A555)

  Directives concerning assets slated for retirement and disposal.

Outputs

- Asset_ Disposed

  Assets that have reached the end of their useful lifecycle and have been removed from service and inventory. Disposal can involve selling, scrapping or recycling.
- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

- Asset_ Reactivated (To: A552)

  An asset that was previously retired, but has been brought back into active service.
- Asset Retirement and Disposal Data (To: A552 A553 A555)

  Data that describes the disposition and status of assets slated for retirement and disposal.

[A557] Report Asset Information

Description

Receive and process requests for asset reports. These can include ad hoc reports or standard reports. Design (if needed), generate, and disseminate asset reports as per request.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.

Inputs

- Asset Contracts and Financial Data (From: A555)

  Business records about an asset and related financial information. This includes data such as asset records, vendor information, asset costs and current value, tax data.
- Asset Register (From: A553)

  The complete set of records in asset information repositories.
- Asset Information or Report Request

  A request to obtain information about a deployed asset. This request specifies whether the information should be in a formal report or simply provided asset data. It covers a range of request types, such as:

  - Need for information on an individual asset
  - A scheduled report
  - A request for an asset analysis report.

Outputs

- Asset Reports

  Ad hoc or standard reports describing assets. These reports may describe one or more selected assets or may summarize data about a set of assets, or possibly all assets.
- Asset Management Activity Data (To: A558)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

[A558] Evaluate Asset Management Performance

Description

This activity assesses the performance of the Asset Management process activities against defined performance criteria and measures, and provides input to the IT Management System Framework.

The evaluation of process performance identifies areas that need improvement. This might include the foundation and interfaces of the process, activity definitions, key performance metrics, the state of supporting automation, as well as the roles and responsibilities and skills required. Insights and lessons learned from direct observation and data collected on process performance are the basis for improvement recommendations.

Controls

- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.

Inputs

- Asset Management Activity Data (From: A552 A553 A554 A555 A556 A557)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall Asset Management process.

Outputs

- Asset Management Evaluation (To: A551)

  Assessment results for the Asset Management process and its activities, including process performance metrics and the identification of potential process improvement items.

PRM-IT A5 Node Tree

A5 – TRANSITION	
A51	**Change Management**
A511	Establish Change Management Framework
A512	Create and Record Change Request
A513	Accept and Categorize Change
A514	Assess Change
A515	Authorize and Schedule Change
A516	Coordinate Change Implementation
A517	Review and Close Change
A518	Monitor and Report Change Management
A519	Evaluate Change Management Performance
A52	**Release Management**
A521	Establish Release Management Framework
A522	Plan Release Strategy
A523	Design and Build Release
A524	Test and Verify Release
A525	Monitor and Report Release
A526	Review and Close Release
A527	Evaluate Release Management Performance
A53	**Deployment Management**
A531	Establish Deployment Management Framework
A532	Plan Deployment Program
A533	Prepare Deployment Capabilities
A534	Perform Deployment
A535	Perform Deployment
A536	Verify Deployment and Activate Service
A537	Review and Close Deployment
A538	Monitor and Report Deployment Program
A539	Evaluate Deployment Management Performance
A54	**Configuration Management**
A541	Establish Configuration Management Framework
A542	Identify Configuration Items
A543	Control Configuration Items
A544	Report Configuration Status
A545	Verify and Audit Configuration Items
A546	Evaluate Configuration Management Performance
A55	**Asset Management**
A551	Establish Asset Management Framework
A552	Ready and Control Asset
A553	Control Asset Information
A554	Monitor, Audit and Reconcile Asset Records

A5 – TRANSITION	
A555	Oversee Asset Contracts and Financials
A556	Retire and Dispose of Asset
A557	Report Asset Information
A558	Evaluate Asset Management Performance

Figure 7. A5 Transition Node Tree

