PRM-IT V3 Reference Library - A6 Operations

PRM-IT Version 3.0

April, 2008

PRM - IT
IBM Process Reference Model for IT

Sequencing the DNA of IT Management

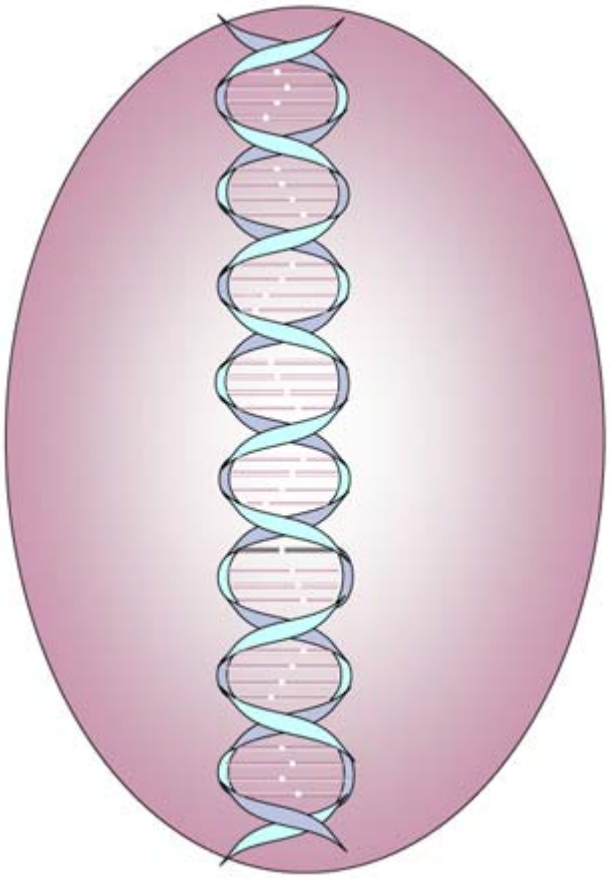

Table of Contents

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 eighth book in the PRM-IT Reference Library. As a reference manual, this book examines the context of the processes for IT, exploring the key external agents and their interactions with IT.

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 aspects 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.

[A6] Operations

Description

Purpose

This category contains the operational service processes that enable daily IT activities using available infrastructure, applications, and services to meet service level agreements (SLAs) and business objectives. Responsibility for delivery of service sits here. Managing contact and communications with users (for example, service requests) is an important function as these processes sense and respond to day-to-day aspects of operations and events, quickly and correctly to address any incidents and problems that might arise.

Rationale

The Operations category comprises all the activities and measures necessary to enable and maintain the intended and committed use of the infrastructure, applications, and services. The processes in this category require close integration to function effectively. Operational plans and workload balancing are augmented by constant operational monitoring throughout service delivery. This operational data is used by many processes to identify, analyze, and quickly resolve any anomalies. The Operations category is also the focal point for receiving and responding to a wide variety of user service requests. This process category is vital to operating organizational constructs such as a Service Desk or an Operations Bridge or an Operations Center. Problem Management is included in this category because of its dependence on incident management information.

Value

- Operates, manages, and maintains an end-to-end infrastructure to facilitate the delivery of the services to the business, meeting all of the agreed to requirements and targets
- Provides sense and respond correction and optimization for any fluctuations within the designed operating characteristics of the IT infrastructure, applications, and services
- Provides a focal point for reliable, robust, secure, and consistent delivery of service, minimizing potential negative impact on the efficiency and effectiveness of business processes
- Establishes responsibility for user contact, service requests and other interactions, improving communications and customer perception of service quality
- Provides the designed level of integrity for data at all stages of its life cycle, including protection of business (and IT) data from accidental loss
- Ensures that any faults or issues are recognized and appropriately addressed

Controls

- IT Financial Reports (From: A8 A81 A813 A814 A815)
- Change Schedule (From: A5 A51 A515 A516)
- Architecture Baselines and Roadmaps (From: A3 A33 A334)
- IT Plan (From: A3 A36 A365)
- Service Catalog (From: A2 A23 A235)
- SLAs, OLAs, UCs (From: A2 A24 A243)
- IT Management Ecosystem (From: A1)
- Security Policy (From: A7 A72 A722)

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

Inputs

- Solution_ Deployed (From: A5 A53 A536)
- Change Information (From: A5 A51 A518)
- Configuration Information (From: A5 A54 A544)
- Solution Design (From: A4 A42 A425)
- Solution Plans and Commitments (From: A4 A41 A42 A422 A425 A43 A432 A44 A442 A45 A452)
- 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)
- User Input (From: Outside-the-Model)
- Service Resilience Plans (From: A7)

Outputs

- User Output (To: Outside-the-Model)
- Identity and Access Rights Register (To: A674 A675 A7 A72 A726 A727 A75 A754)
- Service Metric Data and Reports (To: A2 A24 A244 A7 A71 A716 A8 A81 A814 A815 A83 A832)
- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)
- Incident Information (To: A2 A24 A244 A61 A613 A615 A652 A653 A654 A655 A656 A66 A662 A7 A72 A726 A73 A736 A74 A744 A75 A754)
- Problem Information (To: A2 A24 A244 A245 A356 A61 A613 A615 A65 A653 A654 A656 A662 A663 A664 A665 A666 A7 A73 A736 A74 A744 A76 A764)
- Service Request_ Authorized (To: A5 A53 A535 A55 A552 A62 A622 A63 A67 A7 A72 A75)
- CI Data Update Package (To: A5 A54 A542 A543)
- Change Request (To: A5 A51 A512)

Processes

This process category is composed of these processes:

- A61 Request Fulfillment
- A62 Service Execution
- A63 Data Management
- A64 Event Management
- A65 Incident Management
- A66 Problem Management
- A67 Identity and Access Management

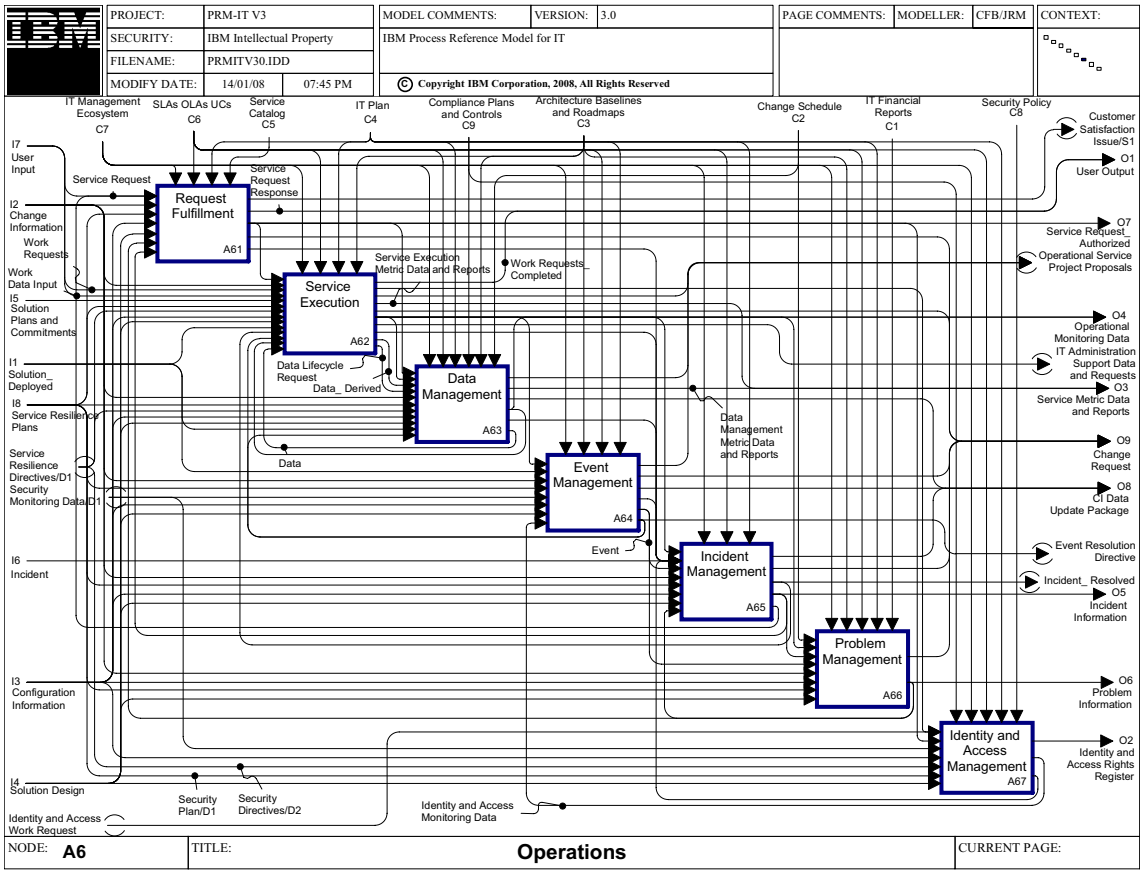

Figure 1. A6 Operations Diagram

[A61] Request Fulfillment

Purpose

The purpose of the Request Fulfillment Process is to receive service requests from users and route each request to the appropriate process for handling. Some service requests are handled by the Request Fulfillment Process, whereas many others are routed to other processes for fulfillment. Request Fulfillment can be the contact management process for an implementation of an IT Service Desk (or equivalent).

Definition of service request: “A request from a user for information, or advice, or for a standard change or for access to an IT service. For example to reset a password, or to provide standard IT services for a new user. Service requests are usually handled by a service desk, and do not require an RFC to be submitted.”[1]

Outcomes

As a result of the successful implementation of the Request Fulfillment Process:

- User and customer satisfaction is enhanced
- User requests to the IT organization are successfully received and processed for fulfillment or other appropriate handling
- Requests are accurately and appropriately routed to the correct process and correct service provider for handling (fulfillment)
- Service level targets for service desk responsiveness and quality are achieved
- Users receive accurate and timely communication concerning the status of their service requests

Scope

At the initial receipt of a service request from a user, the nature of the request and information within it has to be established. Many such service requests can be dealt with by the set of activities within this process. Other service requests, once initially assessed, will be beyond the capability of this process to perform the primary added-value work needed by those requests and will be passed on to other, more specific processes. This process will interact at the process framework level with the specific processes to determine which types of service requests should be handled by which processes. Over time, the range of service requests which can be directly fulfilled is likely to increase.

Examples of interactions are:

- Incidents are routed to the Incident Management process
- Service requests assessed as standard changes are passed directly to other appropriate processes
- Other, more significant change requests are transferred to the Change Management process

Wherever the service request is dealt with, this process retains ownership of the service request on the user's behalf and is responsible for achievement of service level targets relating to service requests.

This process provides the primary interface point for users of IT services with the service provider.

1. ITIL V3 Glossary

Includes

Receipt and management of service requests relating to:

- Incidents
- Standard changes (such as deployment of standard software)
- Identity
- Access rights
- Security service requests
- Information, advice, guidance
- User satisfaction interactions
- Complaints

Items which are assessed to be change requests (rather than standard changes) can be routed to Change Management

Excludes

- Those interactions between the business (and other customers) and the IT service provider that consider the status, scope or coverage of the overall service provision agreements. (Service Level Management)
- The direct fulfillment of those service requests which are dealt with by other processes. Where such fulfillment workings require direct contact between IT service provider staff performing those processes and users, then those activities are part of those processes. An example of this would be interacting with a user as part of deploying a PC (Deployment Management)
- Establishing entitlement limits for user communities against each service (Combination of Service Marketing and Sales, and Service Level Management)
- Granting access rights (found in Identity and Access Management)
- Installing standard technical components (Deployment Management)

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.

- 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."[2]

- 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."[3]
- 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."[4]

These agreements can be in a draft or finalized status.

- 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.

- 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."[5]

Inputs

- Service Request (From: A65 A653)

  A request to perform a standard and straightforward IT task for a user. Service requests are tasks that are within the scope of existing IT services.

  ITIL definition: "A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted."[6]

- 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.

- 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

2. ITIL V3 Glossary
3. ITIL V3 Glossary
4. ITIL V3 Glossary
5. ITIL V3 Glossary
6. ITIL V3 Glossary

- Facilities Management
- IT Service Continuity Management

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

- 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.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

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.

- Service Request Response

  The interim and final outcomes of the service request, which can be many aspects, including:

  - The information requested by the user
  - A request for more information or an acknowledgement of a milestone within the request processing
  - Status of the work effort triggered by the request, including plans to address the work items contained in the request

- Service Request_ Authorized (To: A5 A53 A535 A55 A552 A62 A622 A63 A67 A7 A72 A75)

  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.

- 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.

- 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 service. Incidents can be created using either manual or automated mechanisms. An incident reported by a user begins as a user contact and becomes an incident once it is determined that a fault is being reported.

Activities

This process is composed of these activities:

- A611 Establish Request Fulfillment Framework
- A612 Receive and Approve Service Request
- A613 Fulfill or Route Service Request
- A614 Close Service Request
- A615 Own, Monitor, Track and Communicate Service Requests
- A616 Evaluate Request Fulfillment Performance

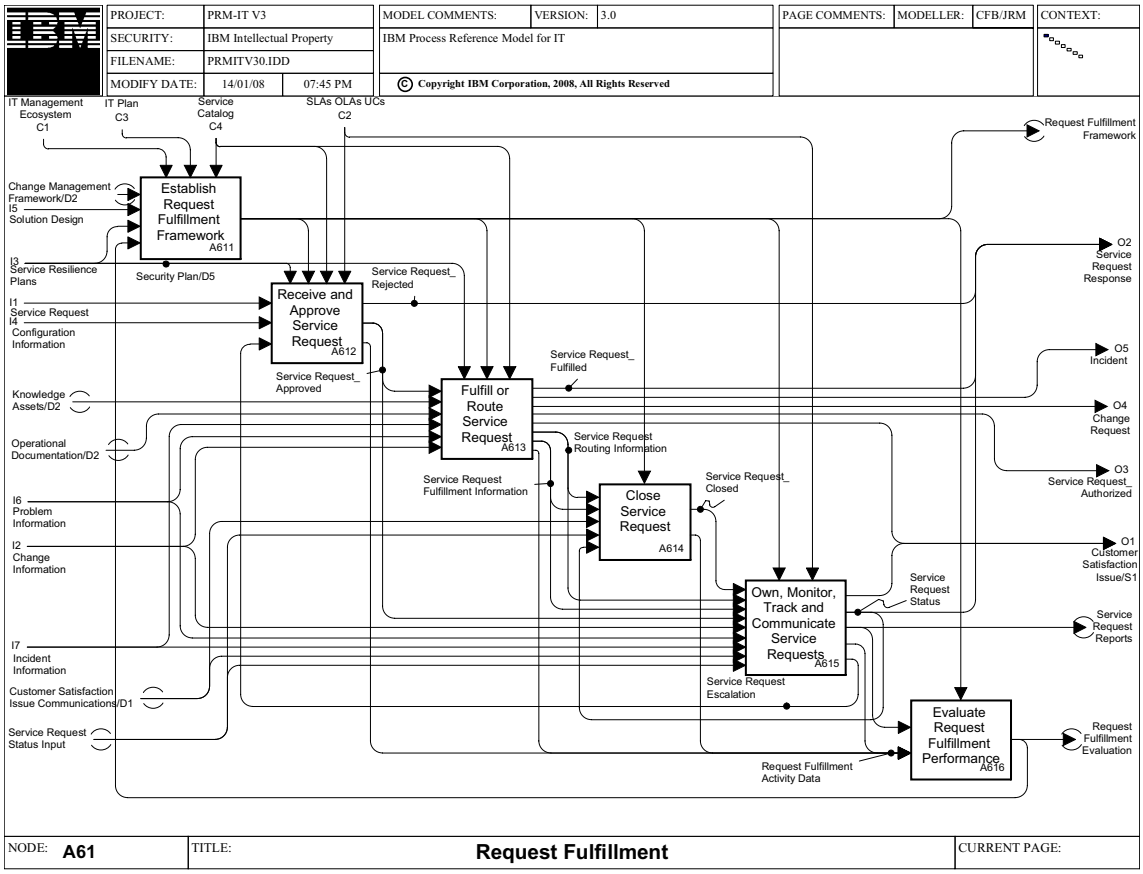

Figure 2. A61 Request Fulfillment

[A611] Establish Request Fulfillment Framework

Description

This activity consists of tasks that establish the base for any request or contact for assistance. This includes several different topics that have to be handled:

- Determine the structure of the logical entity that is the service request center. This should be a single point of contact (SPOC), regionally, locally dispersed, or virtual.
- Define in which format inbound and outbound communication will be done. Meaning, how users can contact the IT service provider (telephone, fax, e-mail, Internet) and how the request fulfillment process communicates with the users.
- Determine the categorization of service requests (standard changes, incidents, service contacts, contacts for advice, and more) and define priorities. Allowance must be made for users submitting requests which, when examined, are determined to be in a category different from that suggested by the user.
- Collect the technology requirements for tooling of request fulfillment. Select and implement tools including relevant procedures. Technology requirements will reflect the range of media (described earlier) and the mix of self-help and service provider delivery.
- Determine which requests can be fulfilled within this process and which requests (once authorized) are to be transferred to other processes.
- Set measurable targets that relate to the agreed SLAs.
- Based on these specifications define skill requirements for the staff (contact handlers) and, if necessary, determine training requirements.
- Finally, communicate the structure and process of request fulfillment to the users.

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.
- 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.
- 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.”[7]

7. ITIL V3 Glossary

Inputs

- 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.

- 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.

- 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.)

- Request Fulfillment Evaluation (From: A616)

  The result of the evaluation of the Request Fulfillment process, including any identification of potential process improvement areas.

Outputs

- Request Fulfillment Framework (To: A612 A613 A614 A615 A616)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Structure of the request fulfillment center (often known as or linked to a *service desk*)
  - Technology support
  - Request routing tables and completion details of request completion targets and commitments
  - Format of information transfer
  - Categorization and prioritization aspects for service requests

  It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

[A612] Receive and Approve Service Request

Description

When a user makes a request for service using one of the available channels (such as by calling a service desk, by sending an e-mail or by completing a self-service dialog), the request is examined and checked to see if it passes the criteria for acceptance. If not, it is rejected.

Typical tasks include:

- Checking completeness and accuracy of user information
- Confirming user entitlement to have the request processed, and perhaps defining a class of service for the request
- Calling up and confirming relevant configuration information.

In order to be able to follow up on the service request later, a reference number is typically assigned to the request and the contact details are stored in a repository (tool or database, depending on the selected tooling for request fulfillment). If the request is rejected, this decision and the reasons are communicated to the user.

Once accepted, the request is classified, meaning that the request handler performs a request assessment. This includes understanding and analyzing the request content so that a categorization is possible as well as a prioritization of the request (based on the rules defined in the request fulfillment framework). Additionally, all relevant information about the request is documented in the request details.

Controls

- Security Plan (From: A72 A725)

  A consolidated view and documentation of the resources, approach, procedures and assets to be protected together with a definition of the security practices and controls which will be enacted in order to fulfill the security policy. It covers both technical capabilities (for example, firewalls, and encryption) and non-technical considerations (such as segregation of duties, training needs, user responsibilities).

- Request Fulfillment Framework (From: A611)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Structure of the request fulfillment center (often known as or linked to a *service desk*)
  - Technology support
  - Request routing tables and completion details of request completion targets and commitments
  - Format of information transfer
  - Categorization and prioritization aspects for service requests

  It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

- 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."[8]

- 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.

Inputs

- Service Request (From: A65 A653)

  A request to perform a standard and straightforward IT task for a user. Service requests are tasks that are within the scope of existing IT services.

  ITIL definition: "A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted."[12]

- 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 Escalation (From: A615)

  Information about a service request that has not been fulfilled in ways that meets satisfaction criteria and which requires escalation.

8. ITIL V3 Glossary
9. ITIL V3 Glossary
10. ITIL V3 Glossary
11. ITIL V3 Glossary
12. ITIL V3 Glossary

Outputs

- Service Request_ Rejected

  A service request that is not accepted as falling into one of the pre-defined categories for requests or which fails the entitlement tests. An example of this would be a new requirement for functionality (for which the user should be guided to invoke the Stakeholder Requirements process).

- Service Request_ Approved (To: A613 A615)

  A service request which has met the classification and entitlement rules and which includes all the information needed for fulfillment. It is ready to be fulfilled or routed.

- Request Fulfillment Activity Data (To: A616)

  Any data about the accomplishment of process activities that support the evaluation of the overall Request Fulfillment process.

[A613] Fulfill or Route Service Request

Description

Depending on the request assessment, the service request can be satisfied within this process (within the remit established by the Request Fulfillment Framework) or routed to other processes.

If the service request is to be fulfilled within the capabilities of this process (for example, by providing information or guidance), the response to the request will be created and documented and sent to the user. Either the service request is resolved (the user is satisfied), or the request handler escalates the issue. The latter can lead to a reconsideration of the request fulfillment approach or to a transfer to other processes (if the request cannot be fulfilled in a satisfying way by the request handler).

If the service request has to be transferred to another process, the request item will be assigned depending on categorization (for example, to Incident Management) or prioritization of the request. This means that the request including all relevant information and documentation (detailed description, any advice, guidance) is routed and the receiving process is notified about the assigned request item.

If the service request is resolved, a check can be made with the user concerning their satisfaction with the resolution, and all relevant information is updated, culminating with marking the service request as ready for closure.

Controls

- Security Plan (From: A72 A725)

  A consolidated view and documentation of the resources, approach, procedures and assets to be protected together with a definition of the security practices and controls which will be enacted in order to fulfill the security policy. It covers both technical capabilities (for example, firewalls, encryption) and non-technical considerations (such as segregation of duties, training needs, user responsibilities).

- Request Fulfillment Framework (From: A611)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Structure of the request fulfillment center (often known as or linked to a service desk)
  - Technology support
  - Request routing tables and completion details of request completion targets and commitments
  - Format of information transfer

- Categorization and prioritization aspects for service requests

It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

- 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]

Inputs

- Service Request_ Approved (From: A612)

  A service request which has met the classification and entitlement rules and which includes all the information needed for fulfillment. It is ready to be fulfilled or routed.

- Knowledge Assets (From: A85 A855)

  Any information from knowledge management that fulfills a knowledge request.

- 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.

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own 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.

Outputs

- Service Request Fulfilled

  A service request that has been fulfilled within the Request Fulfillment process or in the processes to which it had been routed. Is either the actual fulfillment itself (for example, service usage guidance), or just information about the work carried out elsewhere (such as notification of incident resolution or confirmation of software download and installation).

13. ITIL V3 Glossary

- 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.

- 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.

- Service Request_ Authorized (To: A5 A53 A535 A55 A552 A62 A622 A63 A67 A7 A72 A75)

  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.

- 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.

- Service Request Routing Information (To: A614 A615)

  Details of how the work represented by the service request has been assessed and planned for fulfillment by or to be passed to one or more other processes. The details include:

  - The request classification, including the cases where the request has been re-classified as an incident or a change request
  - The process and specific team or individual where the work has been assigned

- Service Request Fulfillment Information (To: A614 A615)

  Information about a service request that has been successfully fulfilled.

- Request Fulfillment Activity Data (To: A616)

  Any data about the accomplishment of process activities that support the evaluation of the overall Request Fulfillment process.

[A614] Close Service Request

Description

This activity describes the tasks involved in reviewing service requests that have been marked for closure. It checks that the service request has had the desired effect and met its objectives, and that *users* and *customers* are content with the results, or to identify any shortcomings. It further examines the work undertaken to fulfill the request and ensures that all data required by the request fulfillment framework is fully and properly captured. The activity determines whether any follow-up action (such as the update of request handling documentation) is required and if not, a formal close of the service request is performed.

Controls

- Request Fulfillment Framework (From: A611)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Structure of the request fulfillment center (often known as or linked to a service desk)
  - Technology support

- Request routing tables and completion details of request completion targets and commitments
- Format of information transfer
- Categorization and prioritization aspects for service requests

It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

Inputs

- Service Request Routing Information (From: A613)

  Details of how the work represented by the service request has been assessed and planned for fulfillment by or to be passed to one or more other processes. The details include:

  - The request classification, including the cases where the request has been re-classified as an incident or a change request
  - The process and specific team or individual where the work has been assigned
- Service Request Fulfillment Information (From: A613)

  Information about a service request that has been successfully fulfilled.
- Customer Satisfaction Issue Communications (From: A27 A274)

  Information provided to customers about any aspect of a satisfaction issue, covering analysis of causes, committed plans to address, and progress to issue resolution.
- Service Request Status Input

  Details, from any process involved in processing the service request, on status and plan to complete the work involved. It can include a request to obtain more information or some form of acknowledgement from the user.
- Service Request Status (From: A615)

  The status of a service request (received, work in progress, resolved, or closed). Used to communicate the information to the user (originator of the request).

Outputs

- Service Request_ Closed (To: A615)

  A service request for which all fulfillment activities have been completed and information about the fulfillment has been captured.
- Request Fulfillment Activity Data (To: A616)

  Any data about the accomplishment of process activities that support the evaluation of the overall Request Fulfillment process.

[A615] Own, Monitor, Track and Communicate Service Requests

Description

Throughout the period of request handling and fulfillment the service request status is monitored for several reasons:

- It must be ensured that the status of the request can be communicated to the originating user at any time.
- The status of the request must be known in order to initiate escalation (according to existing escalation management policies and guidelines) if the current fulfillment status breaches agreed SLAs.

Monitoring the request status not only relates to individual requests, but also to all requests collectively so that the overall compliance with SLAs for request fulfillment as a service or part of a service can be controlled.

Analysis and reporting on the service requests will be carried out on a predetermined basis (weekly, monthly, and when exceptions are indicated) in order to control the quality of request fulfillment, the compliance with existing SLAs, for planning purposes and as a basis for improvements.

Examples of reports to be produced include:

- The number, categories, and sources of requests
- The elapsed time until requests are fulfilled
- The workload per request or per staff member
- Analysis of patterns of potentially avoidable requests that might have been caused through incorrect or inadequate user understanding of service characteristics and features

There will be reports about the availability of the request fulfillment center and the overall compliance with SLAs. Basically, the reports serve as a measure to check if the service requests are handled in a way that complies with the agreed targets.

These reports and their analysis will also help to do some trend analysis and forecasting with regard to service requests, relevant for the planning of staffing and other request fulfillment related topics. The output of this process will also be available to the knowledge management process with the objective of enhancing the effectiveness and efficiency of request fulfillment.

Controls

- Request Fulfillment Framework (From: A611)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Structure of the request fulfillment center (often known as or linked to a service desk)
  - Technology support
  - Request routing tables and completion details of request completion targets and commitments
  - Format of information transfer
  - Categorization and prioritization aspects for service requests

  It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

- 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.

Inputs

- Service Request_ Closed (From: A614)

  A service request for which all fulfillment activities have been completed and information about the fulfillment has been captured.
- Service Request Routing Information (From: A613)

  Details of how the work represented by the service request has been assessed and planned for fulfillment by or to be passed to one or more other processes. The details include:
  - The request classification, including the cases where the request has been re-classified as an incident or a change request
  - The process and specific team or individual where the work has been assigned
- Service Request Fulfillment Information (From: A613)

  Information about a service request that has been successfully fulfilled.
- Service Request_ Approved (From: A612)

  A service request which has met the classification and entitlement rules and which includes all the information needed for fulfillment. It is ready to be fulfilled or routed.
- 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.
- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

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

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- Customer Satisfaction Issue Communications (From: A27 A274)

  Information provided to customers about any aspect of a satisfaction issue, covering analysis of causes, committed plans to address, and progress to issue resolution.

- Service Request Status Input

  Details, from any process involved in processing the service request, on status and plan to complete the work involved. It can include a request to obtain more information or some form of acknowledgement from the user.

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.

- Service Request Status (To: A614)

  The status of a service request (received, work in progress, resolved, or closed). Used to communicate the information to the user (originator of the request).

- Service Request Reports (To: A244 A518 A616)

  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.

- Request Fulfillment Activity Data (To: A616)

  Any data about the accomplishment of process activities that support the evaluation of the overall Request Fulfillment process.

- Service Request Escalation (To: A612)

  Information about a service request that has not been fulfilled in ways that meet satisfaction criteria and which requires escalation.

[A616] Evaluate Request Fulfillment Performance

Description

The evaluation of the performance of the Request Fulfillment process aims at identifying improvement areas of the overall process, such as the foundation and interfaces of the process, all activities, their accomplishment, their degree of automation as well as the roles and responsibilities including the respective skills.

Basis for the improvements are insights and lessons learned that are gained from the reports and their analysis. Basically, the improvements should lead to more efficiency and a better compliance with the SLAs.

Controls

- Request Fulfillment Framework (From: A611)

  The framework that contains all relevant information about the structure of the Request Fulfillment process. For example:

  - Technology support{ Structure of the request fulfillment center (often known as or linked to a service desk)
  - Request routing tables and completion details of request completion targets and commitments
  - Format of information transfer
  - Categorization and prioritization aspects for service requests

  It defines the records which should be kept for each service request containing all relevant details across the life cycle of the request. Information in a record includes data relevant to service provider analysis as well as the details directly relevant to the requestor.

Inputs

- 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.

- Request Fulfillment Activity Data (From: A612 A613 A614 A615)

  Any data about the accomplishment of process activities that support the evaluation of the overall Request Fulfillment process.

Outputs

- Request Fulfillment Evaluation (To: A611)

  The result of the evaluation of the Request Fulfillment process, including any identification of potential process improvement areas.

[A62] Service Execution

Purpose

The purpose of the Service Execution process is to deliver operational services to IT customers, by matching resources to commitments and employing the IT infrastructure to conduct IT operations.

Definition of operation: “Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.”[17]

Outcomes

As a result of the successful implementation of this process:

- Services are delivered in a reliable, robust, secure, and consistent manner
- Services are provided within service level targets
- Resources needed to operate IT services are managed effectively and efficiently
- Consumable resources used to deliver services are supplied in a timely manner
- Up-to-date service metric information is available

Scope

This process is responsible for the scheduling, operation and execution of the IT-based services which have been committed to customers. These services are of many types, including business transaction and batch processing, and also many types of self-service functionality offered as standard services to users.

Service Execution applies the resources made available to it through Deployment Management to the dynamic mix of workload demands. It makes adjustments to resource allocations within the tolerances provided and specified in the solution design.

Includes

- Understanding, creation, and maintenance of operational schedules
- Starting, stopping, and other operational resource management actions on system components, applications and other services
- Monitoring of system resources
- Detecting events and sending significant events to Event Management
- Understanding and maintenance of operational status
- Managing production workloads from submission through delivery of results and from service start to service close

Excludes

- Correlating and processing significant events (Event Management)
- Operational security (Security Management)
- Data management, backup, and recovery (Data Management)

17. ITIL V3 Glossary

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.

- 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.

- 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.

- 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

- 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.

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

- 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.

- Work Requests

  An unqualified request for processing services involving IT resources. To be accepted for processing, it must contain sufficient detail in order to match it against the list of existing services and to determine the characteristics (parameters) of this specific request. Work requests can range from highly granular individual interactions (pressing a function key on a PC) to a large clump of work (a long running batch job, perhaps with many dependent steps and subsequent, dependent jobs).

- Work Data Input

  The data that is submitted along with a work request and which has not yet been processed (so that it becomes *managed data*). It could have been captured in many ways of which keyboard, magnetic card reader, barcode reader, RFID tag are just some examples.

- 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.

- 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.)

- Service Resilience Directives (From: A72 A74 A76)

  The collection of commands, instructions or other requests from Resilience processes to the Operations processes which will lead to an improvement in, or correction of, any aspect of service.

- 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.

- Solution_ Deployed (From: A5 A53 A536)

  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_ Resolved (From: A65 A655)

  An incident for which a workaround or fix has been successfully applied.

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operational service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data (From: A63 A634)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

Outputs

- Work Requests_ Completed

  The results, in terms of data and any confirmation responses, returned to the work requestor upon completion of the triggering request for work to be performed by the IT operational service. This output represents the fundamental item for which the customer is paying; that is, the processing of transactions whether real time or batched.

  Can include negative outcomes, such as unsuccessful processing, resource authorization failure, and resource insufficiency.

- Identity and Access Work Request (To: A67)

  An identity and access request originating from another process.

- Operational Service Project Proposals

  Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:

  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance

- Service Execution Metric Data and Reports

  Significant service execution event logs, volume and other measurement data relating to how effectively and efficiently service execution has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is the basis for service level reporting.

- 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.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- IT Administration Support Data and Requests

  Covers requests for supply of new or additional consumable materials and relevant data reporting on consumption and usage of the consumables (tapes, paper, toner, forms, and others), which might be required for charging.

- 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.

- Data_ Derived (To: A63 A634)

  Any informational item created or modified as part of the workings of any business process and which is to be managed within an IT service. Data could be specific information like order numbers, invoice numbers, receipts, inventory change data, and could be received in batches or in individual transactions. It can relate to business processes, or be relevant to the management of the IT endeavor.

- Data Lifecycle Request (To: A63 A632 A634 A636)

  The identification of any need for a lifestyle management action of any data item as part of productive usage of that data.

Activities

This process is composed of these activities:

- A621 Establish Service Execution Framework
- A622 Schedule and Adjust Workload
- A623 Assign and Control Delivery Resources
- A624 Deliver Service
- A625 Monitor and Report Service Execution Operations
- A626 Evaluate Service Execution Performance

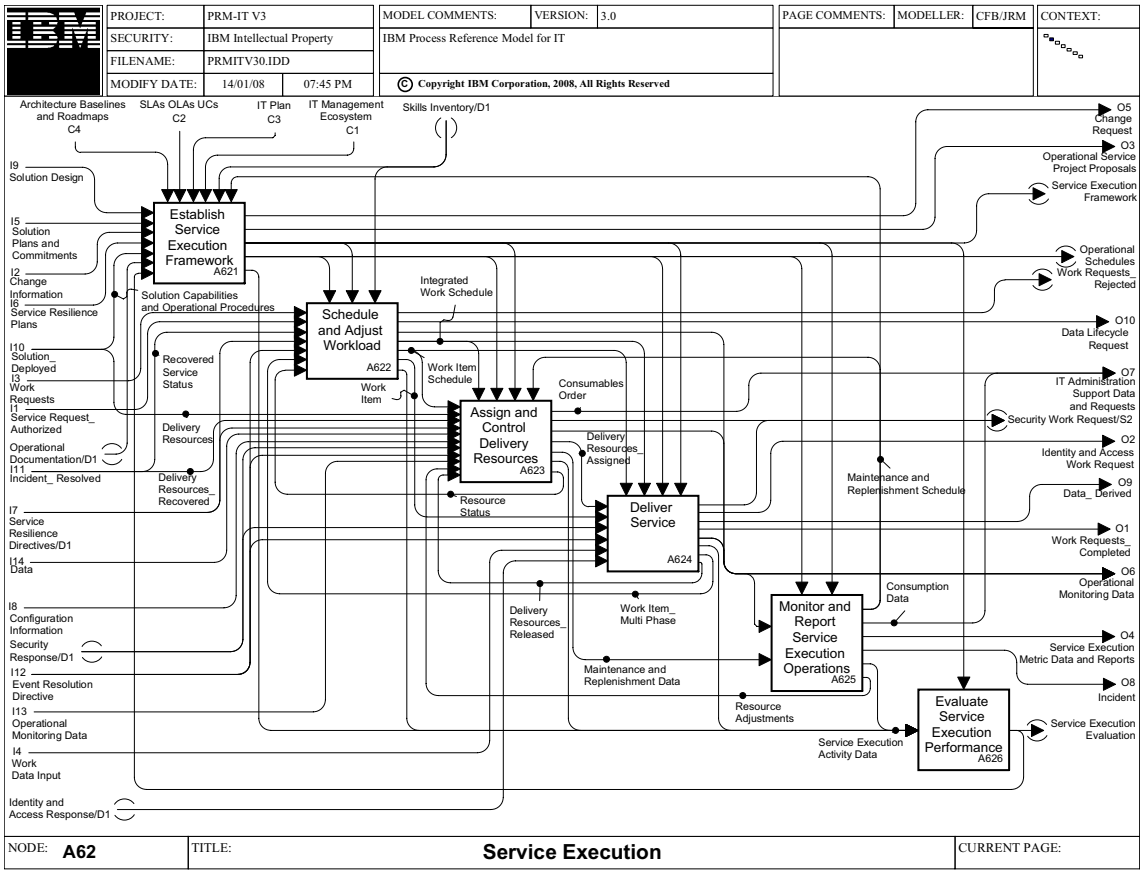

Figure 3. A62 Service Execution

[A621] Establish Service Execution Framework

Description

This is the activity of defining and documenting the rules and policies governing day-to-day service execution activities. The purpose of this activity is the creation of a working framework geared to deliver agreed services to the customer of information technology. All services must meet expected quality, be within budget, and in such a way as to produce a high degree of customer satisfaction while keeping to the IT strategy.

Controls

- 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.

- 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.”[21]
  - 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.”[22]
  - 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.”[23]

  These agreements can be in a draft or finalized status.

- 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.

21. ITIL V3 Glossary
22. ITIL V3 Glossary
23. ITIL V3 Glossary

- Skills Inventory (From: A844)

  Repository for current and planned skills.

- Maintenance and Replenishment Schedule (From: A625)

  The time, date, quantity and other related information relating to the maintenance of delivery resources and to the re-supply of consumable materials.

Inputs

- 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.

- 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.

- 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 Capabilities and Operational Procedures

  The capabilities and operational procedures deployed as part of current solutions. These might require further development and tuning in order to reach optimal effectiveness as part of Service Execution.

  (Subset of *Solution 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.

- Service Execution Evaluation (From: A626)

  A report or data providing measurements, trending and metrics on the health and performance of Service Execution. Includes identification of potential process improvement areas.

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.
- Operational Service Project Proposals
- Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:
  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance
- Service Execution Framework (To: A622 A623 A624 A625 A626)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:
  - Operational Procedures
  - Service Execution Plan
- Operational Schedules (To: A51 A515 A52 A521 A522 A53 A532 A622 A623 A624 A625 A743)

  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).
- Service Execution Activity Data (To: A626)

  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.

[A622] Schedule and Adjust Workload

Description

This activity operates at both a macro and micro-level to prepare work schedules, and to preprocess work items where necessary so that they are ready for actual processing. It operates in concert with the activity that ensures the delivery resources can be matched to the demands of the flow of work in an optimal fashion.

Controls

- 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).
- Service Execution Framework (From: A621)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:
  - Operational Procedures
  - Service Execution Plan

- Skills Inventory (From: A844)

  Repository for current and planned skills.

Inputs

- Work Requests

  An unqualified request for processing services involving IT resources. To be accepted for processing, it must contain sufficient detail in order to match it against the list of existing services and to determine the characteristics (parameters) of this specific request. Work requests can range from highly granular individual interactions (pressing a function key on a PC) to a large clump of work (a long running batch job, perhaps with many dependent steps and subsequent, dependent jobs).

- 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.

- Recovered Service Status

  Status information on the recovered service.

- Service Resilience Directives (From: A72 A74 A76)

  The collection of commands, instructions or other requests from Resilience processes to the Operations processes which will lead to an improvement in, or correction of, any aspect of service.

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Work Item_ Multi Phase (From: A624)

  A partially-completed output created by Deliver Services that flows internally within the process. The output would signify that other service execution activities would need to be started. An example of this complex work item is a payroll application: a new employee is added, the new employee can create a new work item to add a new person to an enterprise employee directory. The directory update service is triggered by the payroll addition service.

- Resource Status (From: A623)

  Information pertaining to the status of any IT resource that is used in the provision of service. The status could be available, not available, failing, over-utilized, approaching peak usage, and would include actual status and predictive information for ensuring adequate availability of resources at all times. This also includes Resource Commit Failure.

Outputs

- Rejected Work Requests

  Notification that the request does not comply with work request acceptance criteria, and therefore was rejected.

- Data Lifecycle Request (To: A63 A632 A634 A636)

  The identification of any need for a life cycle management action of any data item as part of productive usage of that data.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Integrated Work Schedule (To: A623 A624)

  A consolidation of all individual work item schedules (planned out sequence of work) based on resources, commitments, skills and available services.
- Work Item Schedule (To: A623 A624)

  Control information on the combination of the work item, the required IT resources, and the timing parameters and instructions which enable matching of work demands with resource supply.
- Work Item (To: A624)

  The basic unit of work of an IT service or work request, ready to be processed.
- Service Execution Activity Data (To: A626)

  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.

[A623] Assign and Control Delivery Resources

Description

This activity assigns, monitors, and adjusts IT delivery resources on a real-time basis against the current mix of workload that has been requested. It applies the appropriate resources, from those available and within their capacity and other operational characteristic limitations, to be ready to deliver and execute those workload requests. It also works to optimize the output capability of each resource by, for example, carrying out resource housekeeping and maintenance when indicated.

Controls

- Integrated Work Schedule (From: A622)

  A consolidation of all individual work item schedules (planned out sequence of work) based on resources, commitments, skills and available services.
- 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).
- Service Execution Framework (From: A621)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:

  - Operational Procedures
  - Service Execution Plan
- Maintenance and Replenishment Schedule (From: A625)

  The time, date, quantity and other related information relating to the maintenance of delivery resources and to the re-supply of consumable materials.

Inputs

- Work Item Schedule (From: A622)

  Control information on the combination of the work item, the required IT resources, and the timing parameters and instructions which enable matching of work demands with resource supply.
- Delivery Resources

  Technological and people resources which can be utilized in the process of delivering IT services to the organization.

- Delivery Resources_ Recovered

  Any IT delivery resources which have been restored to normal (or acceptable) operational capability as a result of incident resolution.

- Service Resilience Directives (From: A72 A74 A76)

  The collection of commands, instructions or other requests from Resilience processes to the Operations processes which will lead to an improvement in, or correction of, any aspect of service.

- Data (From: A63 A634)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

- 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.

- 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 – success or failure of the request

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Resource Adjustments (From: A625)

  Adjustments to IT technical resources that might be required to optimize service execution as a result of analysis of the service execution data, workload, and so forth.

- Delivery Resources_ Released (From: A624)

  Resources (tapes, storage devices, networks, LANS, programs, data stores, processors, memory) that have been used in the process of performing operational services but are now available for re-assignment to other work.

Outputs

- Consumables Order

  An order for materials used up in the process of providing agreed-to services. Materials like paper, magnetic tape, printer toner or ribbons, and others are included.

- Security Work Request (To: A72)

  A Security Request originating from another process.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Delivery Resources_ Assigned (To: A624)

  All IT resources required and available to perform the required service.

- Maintenance and Replenishment Data (To: A625)

  Information pertaining to maintenance activities and to restocking consumable resources. This data could include resource name, amount replenished, location, vendor, and other information.

- Service Execution Activity Data (To: A626)

  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.

- Resource Status (To: A622)

  Information pertaining to the status of any IT resource that is used in the provision of service. The status could be available, not available, failing, over-utilized, approaching peak usage, and would include actual status and predictive information for ensuring adequate availability of resources at all times. This also includes Resource Commit Failure.

[A624] Deliver Service

Description

This activity processes work items through the series of value-added actions which constitute the requested service. It employs the appropriate combination of human and technology resources necessary to perform those actions. It delivers the work results, both final data and processing log, to the specified destinations.

Controls

- Work Item Schedule (From: A622)

  Control information on the combination of the work item, the required IT resources, and the timing parameters and instructions which enable matching of work demands with resource supply.

- Integrated Work Schedule (From: A622)

  A consolidation of all individual work item schedules (planned out sequence of work) based on resources, commitments, skills and available services.

- 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).

- Service Execution Framework (From: A621)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:

  - Operational Procedures
  - Service Execution Plan

Inputs

- Delivery Resources_ Assigned (From: A623)

  All IT resources required and available to perform the required service.

- Work Item (From: A622)

  The basic unit of work of an IT service or work request, ready to be processed.

- 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 – success or failure of the request

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Work Data Input

  The data that is submitted along with a work request and which has not yet been processed (so that it becomes managed data). It could have been captured in many ways of which keyboard, magnetic card reader, barcode reader, RFID tag are just some examples.

- Identity and Access Response (From: A673 A674)

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

  - For an identiy 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

Outputs

- 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.

- Data_ Derived (To: A63 A634)

  Any informational item created or modified as part of the workings of any business process and which is to be managed within an IT service. Data could be specific information like order numbers, invoice numbers, receipts, inventory change data, and could be received in batches or in individual transactions. It can relate to business processes, or be relevant to the management of the IT endeavor.

- Work Requests_ Completed

  The results, in terms of data and any confirmation responses, returned to the work requestor upon completion of the triggering request for work to be performed by the IT operational service. This output represents the fundamental item for which the customer is paying; that is, the processing of transactions whether real time or batched.

  Can include negative outcomes, such as unsuccessful processing, resource authorization failure, and resource insufficiency.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Service Execution Activity Data (To: A626)

  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.

- Work Item_ Multi Phase (To: A622)

  A partially-completed output created by Deliver Services that flows internally within the process. The output would signify that other service execution activities would need to be started. An example of this complex work item is a payroll application: a new employee is added, the new employee can create a new work item to add a new person to an enterprise

employee directory. The directory update service is triggered by the payroll addition service.

- Delivery Resources_ Released (To: A623)

  Resources (tapes, storage devices, networks, LANS, programs, data stores, processors, memory) that have been used in the process of performing operational services but are now available for re-assignment to other work.

[A625] Monitor and Report Service Execution Operations

Description

Examines all monitoring data from the operational delivery tasks within Service Execution and analyzes it against targets to identify any requirement for intervention. Intervention possibilities include within-guidelines resource adjustments and signaling to invoke Incident Management for circumstances that cannot be addressed within this process.

The analysis also provides the basis for reporting (as defined by the framework). These reports could include attainments, trending, and the identification of current and potential issues, as well as the production of the service metric data required by many Service Management processes.

Controls

- 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).

- Service Execution Framework (From: A621)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:

  - Operational Procedures
  - Service Execution Plan.

Inputs

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Maintenance and Replenishment Data (From: A623)

  Information pertaining to maintenance activities and to restocking consumable resources. This data could include resource name, amount replenished, location, vendor, and other information.

Outputs

- Maintenance and Replenishment Schedule (To: A621 A623)

  The time, date, quantity and other related information relating to the maintenance of delivery resources and to the re-supply of consumable materials.

- Consumption Data

  Usage statistics for consumable supplies reported with each use and intended to be the basic information that would lead the IT organization to know when consumables are nearing depletion so the material can be re-supplied without disruption to processing.

- Service Execution Metric Data and Reports

  Significant service execution event logs, volume and other measurement data relating to how effectively and efficiently service execution has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is the basis for service level reporting.

- 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.

- Service Execution Activity Data (To: A626)

  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.

- Resource Adjustments (To: A623)

  Adjustments to IT technical resources that might be required to optimize service execution as a result of analysis of the service execution data, workload, and so forth.

[A626] Evaluate Service Execution Performance

Description

This activity evaluates the current performance of the Service Execution process against the established Service Execution Framework. Specific feedback is provided to the Service Execution Framework to help tune the overall effectiveness and efficiency of Service Execution.

The evaluation of process performance identifies areas that need improvement; such as 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

- Service Execution Framework (From: A621)

  The overall scheme of documents, plans, processes, and procedures designed to govern and optimize all activities for Service Execution. The framework includes:

  - Operational Procedures
  - Service Execution Plan.

Inputs

- Service Execution Activity Data (From: A621 A622 A623 A624 A625)

  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

- Service Execution Evaluation (To: A621)

  A report or data providing measurements, trending and metrics on the health and performance of Service Execution. Includes identification of potential process improvement areas.

[A63] Data Management

Purpose

The purpose of the Data Management process is to ensure that all data necessary in providing and supporting business and operational services is available for use and is actively managed from creation and introduction until final disposal or destruction.

Outcomes

As a result of successful implementation of this process:

- Data life cycle management policies and governance capabilities are effectively provided
- Data life cycle management services are sustained in order to meet or exceed service level commitments
- Legal, regulatory, and business requirements are met for data privacy, quality, and retention
- The accessibility, performance, cost, and value characteristics of data are established, managed and optimized throughout the full life cycle
- The integrity of data at all stages of its life cycle is ensured, including protection of business (and IT) data from accidental loss and destruction

Scope

Management of the full life cycle of both externally acquired and enterprise generated data, as well as information about that data.

Includes

- Managing data as a portfolio and the overall plan for the portfolio's elements
- Cataloging and controlling all data types, such as:
  - Business data
  - Journals and logs
  - Program libraries
  - Systems management data
- Accepting and cataloguing new data
- Planning and control of data placement, retention, and disposalData backup and restoration of data to prior states

Excludes

- Information management activities:
  - Data typing and classification (Architecture Management)
  - Content management (Business responsibility, as part of each business process)
- Change management
- Access control and security protection (Identity and Access Management, Security Management)
- Configuration Management

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.

- 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.”[24]
  - 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.”[25]
  - 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.”[26]

  These agreements can be in a draft or finalized status.

- 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.

- 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.

24. ITIL V3 Glossary
25. ITIL V3 Glossary
26. ITIL V3 Glossary

- 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.”[27]

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.

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data_ Derived (From: A62 A624)

  Any informational item created or modified as part of the workings of any business process and which is to be managed within an IT service. Data could be specific information like order numbers, invoice numbers, receipts, inventory change data, and could be received in batches or in individual transactions. It can relate to business processes, or be relevant to the management of the IT endeavor.

- Data Lifecycle Request (From: A62 A622)

  The identification of any need for a life cycle management action of any data item as part of productive usage of that data.

- 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.

- 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.)

- Service Resilience Directives (From: A72 A74 A76)

  The collection of commands, instructions or other requests from Resilience processes to the Operations processes which will lead to an improvement in, or correction of, any aspect of service.

- 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.

27. 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_ Deployed (From: A5 A53 A536)

  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.

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

Outputs

- Operational Service Project Proposals
- Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:
  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance
- Data Management Metric Data and Reports (To: A632 A634)

  Significant event logs, volume and other measurement data relating to how effectively and efficiently data and storage work has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is a basis for service level reporting.

- 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

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- 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.

- Data (To: A62 A623 A635 A636)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

Activities

This process is composed of these activities:

- A631 Establish Data Management Framework
- A632 Plan Data Portfolio Lifecycle
- A633 Acquire and Prepare Data
- A634 Control, Deploy and Maintain Data
- A635 Backup and Restore Data
- A636 Dispose of Data
- A637 Monitor and Report Data Management Operations
- A638 Evaluate Data Management Performance

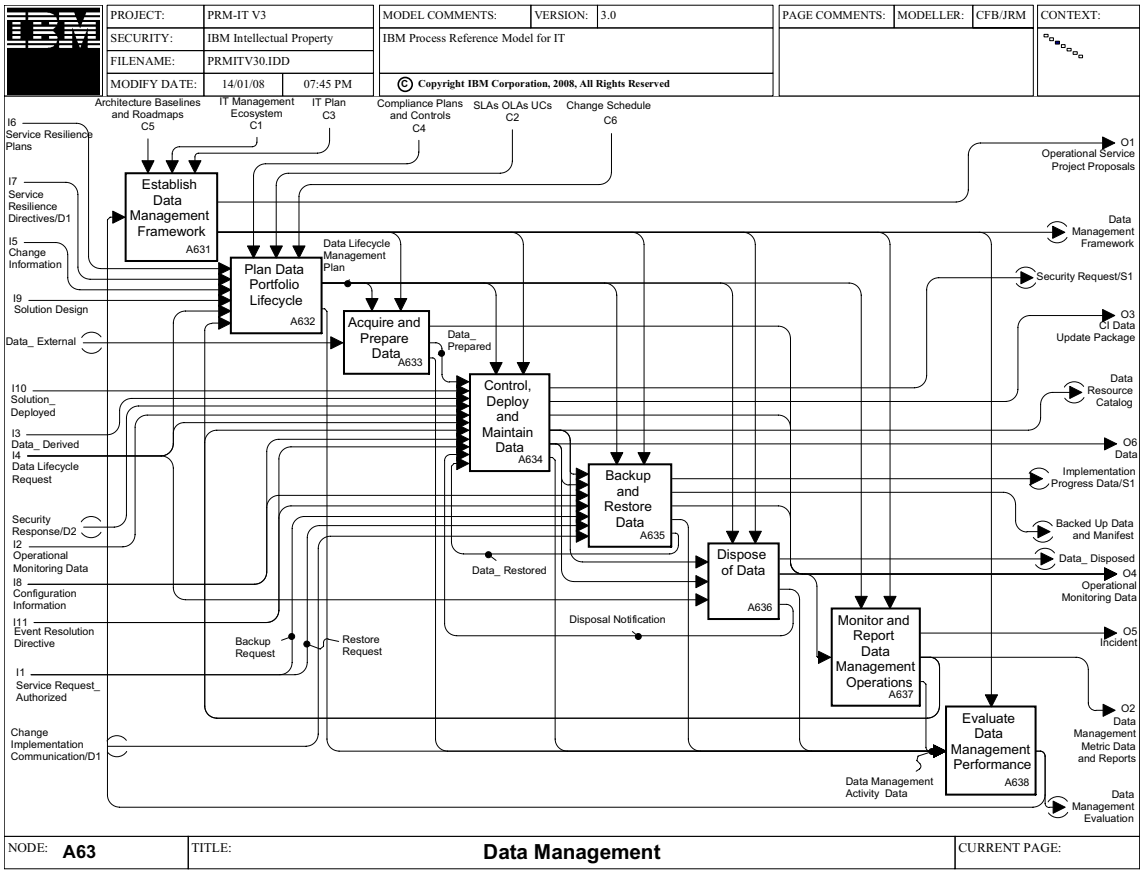

Figure 4. A63 Data Management

[A631] Establish Data Management Framework

Description

Define and maintain a framework of policies and procedures that guides and governs the behavior of the Data Management process and its activities.

Incorporate mandatory elements from the IT Management Ecosystem.

Define a set of measures to be used by each process for measurement and reporting of 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

- 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 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.

Inputs

- Data Management Evaluation (From: A638)

  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

- Operational Service Project Proposals
- Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:
  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance
- Data Management Framework (To: A633 A634 A635 A636 A637 A638)

  The Data Management Framework guides the operation of the process, and includes the following information:
  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)

- Data life cycle models
- General approach to what storage media types will be used for which classes of data
- Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
- Capacity Management plans that affect Data Management
- Data Management requirements based on existing SLAs
- High-level plans for improvement

[A632] Plan Data Portfolio Lifecycle

Description

Identify each candidate collection of data.

Determine the life cycle management requirements and characteristics of each candidate.

Analyze the current portfolio of data and data practices to identify suitable existing practices and needs for new and modified life cycle practices.

Plan the life cycle management scheme for each collection of data.

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.

- 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.”[28]
  - 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.”[29]

28. 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.”[30]

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.”[31]

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.)

- Service Resilience Directives (From: A72 A74 A76)

  The collection of commands, instructions or other requests from Resilience processes to the Operations processes which will lead to an improvement in, or correction of, any aspect of service.

- 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.

- 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.

- Data Lifecycle Request (From: A62 A622)

  The identification of any need for a life cycle management action of any data item as part of productive usage of that data.

- Data Management Metric Data and Reports (From: A63 A637)

  Significant event logs, volume and other measurement data relating to how effectively and efficiently data and storage work has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is a basis for service level reporting.

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

Outputs

- Data Lifecycle Management Plan (To: A633 A634 A635 A636 A637)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification
- Data Management Activity Data (To: A638)

  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.

[A633] Acquire and Prepare Data

Description

Obtain or receive a data collection (per schedule).

Convert, transform or otherwise prepare (extract, clean up) the data.

Package the data.

Controls

- Data Lifecycle Management Plan (From: A632)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification
- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
  - Data life cycle models
  - General approach to what storage media types will be used for which classes of data
  - Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
  - Capacity Management plans that affect Data Management
  - Data Management requirements based on existing SLAs
  - High-level plans for improvement

Inputs

- Data_ External

  Data sourced and obtained from outside the current service coverage. Examples of this would include:

  - Reference data, from external providers, such as postal coding schemes
  - Transaction data from external partners, such as banks

Outputs

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data_ Prepared (To: A634)

  Data that has been collected (acquired) and prepared (filtered, grouped, reordered, rearranged) to match the planned usage. Prepared data is ready to be placed (deployed) onto its target media and managed throughout its life cycle.

- Data Management Activity Data (To: A638)

  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.

[A634] Control, Deploy and Maintain Data

Description

The site or place the data is located, which invokes the Security process for applying the required protections.

Catalog the data, and maintain it with other life cycle activities for which notification is received.

Maintain the data's operational characteristics throughout its deployment.

Migrate data when indicated by policy. The types of migration include from one technology to another, and across locations and system images.

Archive data.

Controls

- Data Lifecycle Management Plan (From: A632)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification

- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

- Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
- Data life cycle models
- General approach to what storage media types will be used for which classes of data
- Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
- Capacity Management plans that affect Data Management
- Data Management requirements based on existing SLAs
- High-level plans for improvement

Inputs

- Data_ Prepared (From: A633)

  Data that has been collected (acquired) and prepared (filtered, grouped, reordered, rearranged) to match the planned usage. Prepared data is ready to be placed (deployed) onto its target media and managed throughout its life cycle.

- Solution_ Deployed (From: A5 A53 A536)

  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.

- Data_ Derived (From: A62 A624)

  Any informational item created or modified as part of the workings of any business process and which is to be managed within an IT service. Data could be specific information like order numbers, invoice numbers, receipts, inventory change data, and could be received in batches or in individual transactions. It can relate to business processes, or be relevant to the management of the IT endeavor.

- 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 – success or failure of the request

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data Lifecycle Request (From: A62 A622)

  The identification of any need for a life cycle management action of any data item as part of productive usage of that data.

- Data Management Metric Data and Reports (From: A63 A637)

  Significant event logs, volume and other measurement data relating to how effectively and efficiently data and storage work has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is a basis for service level reporting.

- 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.

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Disposal Notification (From: A636)

  Notification that one or more collections of data have been disposed of and are no longer accessible.

- Data_ Restored (From: A635)

  Availability of data for productive or other use as a result of restoring it.

Outputs

- Security Request (To: A726)

  System or external request to secure IT resources or validate authority for access.

  - Secure IT resources: identifies one or more specific resources which need to be included in the security protection scheme, or need to have their level and means of protection adjusted
  - Request to access: a communication soliciting access to a particular resource or class of 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.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data Resource Catalog (To: A635 A636)

  The master record of the location and disposition of every data collection under data management. Depending on the policy choices as specified within the framework, it can include usage records such as space employed and lists of users (people, programs) by time and date.

- Data (To: A62 A623 A635 A636)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

- Data Management Activity Data (To: A638)

  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.

[A635] Backup and Restore Data

Description

This activity provides for the local and remote backup and restoration of data from one storage medium to another. It includes replication of data from like storage to like storage and is primarily used to satisfy availability and disaster recovery requirements.

Controls

- Data Lifecycle Management Plan (From: A632)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification

- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
  - Data life cycle models
  - General approach to what storage media types will be used for which classes of data
  - Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
  - Capacity Management plans that affect Data Management
  - Data Management requirements based on existing SLAs
  - High-level plans for improvement

Inputs

- Data Resource Catalog (From: A634)

  The master record of the location and disposition of every data collection under data management. Depending on the policy choices as specified within the framework, it can include usage records such as space employed and lists of users (people, programs) by time and date.

- Data (From: A63 A634)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

- 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.

- Event Resolution Directive (From: A64 A645)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

- Backup Request

  Service Requests from any user or other process that a backup be taken.

- Restore Request

  Service Requests from any user or other process for a data restore to be performed.

- 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

- Implementation Progress Data (To: A51 A516 A537)

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

- Backed Up Data and Manifest (To: A765 A766)

  The data which is the result of taking a backup, in whatever format (for example, compressed, incremental) which has been selected as the basis for any subsequent restore action, plus the indexes and inventories (the manifest) of the content with regard to specific file placement on backup media.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data Management Activity Data (To: A638)

  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.

- Data_ Restored (To: A634)

  Availability of data for productive or other use as a result of restoring it.

[A636] Dispose of Data

Description

Destroy or delete the data so that it is no longer stored and cannot again be accessed. The disposal technique will vary in terms of completeness of data destruction in line with the designation of data sensitivity.

Provide notification so that the data resource catalog can be updated to reflect the disposal.

Controls

- Data Lifecycle Management Plan (From: A632)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification

- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
  - Data life cycle models
  - General approach to what storage media types will be used for which classes of data
  - Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
  - Capacity Management plans that affect Data Management
  - Data Management requirements based on existing SLAs
  - High-level plans for improvement

Inputs

- Data Resource Catalog (From: A634)

  The master record of the location and disposition of every data collection under data management. Depending on the policy choices as specified within the framework, it can include usage records such as space employed and lists of users (people, programs) by time and date.

- Data (From: A63 A634)

  All the data items which are being managed within the IT endeavor, and which are made available for processing or other purposes in line with service commitments.

- Data Lifecycle Request (From: A62 A622)

  The identification of any need for a life cycle management action of any data item as part of productive usage of that data.

Outputs

- Data_ Disposed

  The data that has been taken out of active management. Depending on how it has been stored, it can include the associated media; for example, paper or microfiche records.

- Operational Monitoring Data (To: A62 A623 A625 A63 A634 A637 A64 A642 A65 A654 A655 A66 A662 A7 A73 A735 A74 A743)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Data Management Activity Data (To: A638)

  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.

- Disposal Notification (To: A634)

  Notification that one or more collections of data have been disposed of and are no longer accessible.

[A637] Monitor and Report Data Management Operations

Description

Monitor all aspects of Data Management, including:

- State changes of each and every collection of data
- Matching data status against policies in case action is required (for example, to trigger migration of data between media)

Identify activity which has resulted in data not matching its expected operational characteristics and raise incidents as necessary.

Create data management metrics, including trend data, and reports. Reports can be regular or ad hoc, as circumstances occur.

Controls

- Data Lifecycle Management Plan (From: A632)

  The specification of the life cycle management plan for each class or type of data, allowing for the possibility that an individual collection of data could have unique life cycle management requirements. The life cycle plan will cover aspects such as:

  - Media types to be used, for each activity level of data (such as currency)
  - Archive parameters
  - Backup plan
  - Selection of data sensitivity classification

- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
  - Data life cycle models
  - General approach to what storage media types will be used for which classes of data
  - Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
  - Capacity Management plans that affect Data Management
  - Data Management requirements based on existing SLAs
  - High-level plans for improvement

Inputs

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

Outputs

- 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.

- Data Management Metric Data and Reports (To: A632 A634)

  Significant event logs, volume and other measurement data relating to how effectively and efficiently data and storage work has been performed. This data, which is available as requested both in raw format and as structured reports, is a component of all Operations Information and is a basis for service level reporting.

- Data Management Activity Data (To: A638)

  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.

[A638] Evaluate Data Management Performance

Description

This activity is designed to measure the effectiveness and efficiency of different aspects of the Data Management process, by ensuring that all the necessary information necessary for its management is available for making informed decisions related to the process.

The evaluation of process performance identifies areas that need improvement. This includes 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

- Data Management Framework (From: A631)

  The Data Management Framework guides the operation of the process, and includes the following information:

  - Classes of data (relevant for data management, to indicate factors such as backup scope and frequency)
  - Data life cycle models
  - General approach to what storage media types will be used for which classes of data
  - Instructions for data retention that implement Corporate policies and controls (which themselves include the impact of regulatory requirements)
  - Capacity Management plans that affect Data Management
  - Data Management requirements based on existing SLAs
  - High-level plans for improvement

Inputs

- Data Management Activity Data (From: A632 A633 A634 A635 A636 A637)

  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

- Data Management Evaluation

  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.(To: A631)

[A64] Event Management

Purpose

The purpose of the Event Management process is to identify and prioritize infrastructure, service, business process and security events, and to establish the appropriate response to those events, especially responding to conditions that could lead to potential faults or incidents.

Definition of event: “A change of state which has significance for the management of a configuration item or IT service. The term event is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to Incidents being logged.”[32]

Outcomes

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

- Service quality is sustained and improved
- Incidents are detected early
- The time between event occurrence and detection is minimized
- Appropriate actions are taken in response to events, in order to resolve some without manual response
- Responses to understood faults are started with minimal delay

Scope

Event Management is accomplished through scanning monitoring data and from this collecting, evaluating, responding to, and reporting events throughout the business.

Not all events require a response, only those deemed significant events. Typically, a response to a significant event involves either a predefined response or the creation of an incident in the Incident Management process.

Includes

- Providing both real time and historical event information to other IT processes, to facilitate service quality improvement and resource availability
- Providing similar information relating to the automated aspects of business processes for business analysis
- Correlation and filtering of events, to identify alert notifications and other conditions
- Examination and analysis of individual events in isolation as well as events in context with other events
- Creation of incidents from event information
- Capture, logging and administration of data generated by the activities within this process

Excludes

- System monitoring – Monitoring all things that happen related to a system, whereas event management identifies meaningful changes of state that can represent faults.[33] System monitorig takes place in Service Execution and Data Management.

32. ITIL V3 Glossary

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.

- 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.”[34]
  - 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.”[35]
  - 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.”[36]

  These agreements can be in a draft or finalized status.

- 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.

Inputs

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

33. ITIL *Service Operation*, 36
34. ITIL V3 Glossary
35. ITIL V3 Glossary
36. ITIL V3 Glossary

- Solution_ Deployed (From: A5 A53 A536)

  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.
- 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.
- 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.)
- Security Monitoring Data (From: A72 A726)

  Information relating to the overall item-by-item outcomes from, and status of, security. This can include details of access requests, authentications processed, attacks received and warning thresholds triggered.
- 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.
- Identity and Access Monitoring Data (From: A67 A673 A674)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.

Outputs

- Operational Service Project Proposals
- Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:
  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance
- 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.

- 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.

- Event (To: A643 A65 A654 A66 A662)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[37]

- Event Resolution Directive (To: A62 A622 A623 A624 A63 A634 A635)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.

Activities

This process is composed of these activities:

- A641 Establish Event Management Framework
- A642 Detect and Log Event
- A643 Filter Event
- A644 Correlate Events and Select Response
- A645 Resolve Event
- A646 Close Event
- A647 Evaluate Event Management Performance

37. ITIL V3 Glossary

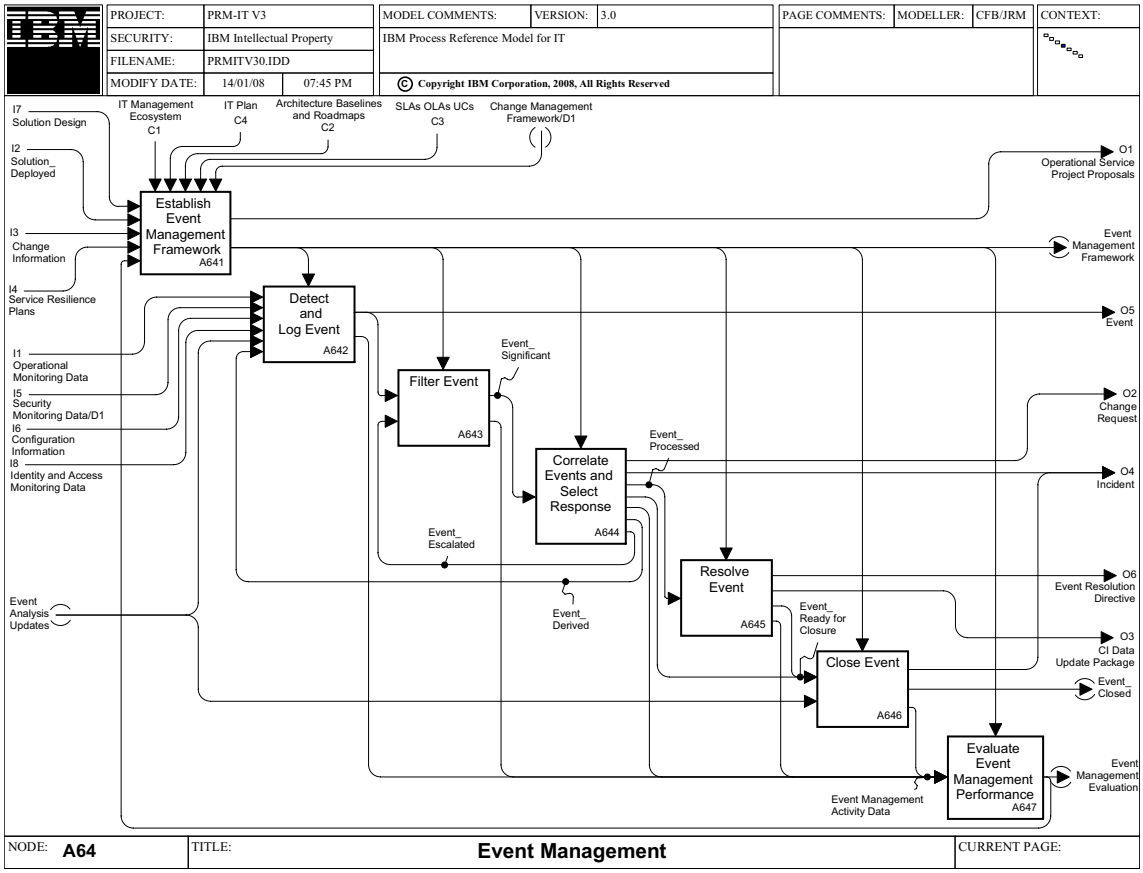

Figure 5. A64 Event Management

[A641] Establish Event Management Framework

Description

Based on the business and IT strategy and the architectural models, guidelines and a framework for Event Management have to be developed. The tasks in this activity include:

- Understanding the requirements and specifications for Event Management
- Defining the strategy for event solutions over and above those provided within individual solutions. For example, should they be developed in-house or rely more on vendor capabilities
- Defining evaluation criteria for event solutions and services
- Establishing the framework for Event Management by defining and implementing practices and systems that support process activities
- Based on these capabilities, determining skill requirements for the staff and assigning staff

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

The establishment of the process framework also includes the continuous improvement of Event Management: the consideration of the Event Management process evaluation and the implementation of recommended improvement actions.

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.

- 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.

- 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.

- 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.”[38]
  - 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.”[39]
  - 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.”[40]

  These agreements can be in a draft or finalized status.

- 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

- 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.

38. ITIL V3 Glossary
39. ITIL V3 Glossary
40. ITIL V3 Glossary

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_ Deployed (From: A5 A53 A536)

  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.

- 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.

- 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.)

- Event Management Evaluation (From: A647)

  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

- Operational Service Project Proposals
- Proposals, from the Framework activities within the Operations category, for project funding. The proposals will go to the Portfolio Management process for decision. The proposal content will be for purposes such as:
  - To establish additional or improved capabilities for performing any activities or tasks within the process
  - To satisfy the operational needs of new technical solutions coming on-stream
  - To improve any relevant aspect of service performance
- Event Management Framework (To: A642 A643 A644 A645 A646 A647)

  Includes the following:

  - Specification of what makes an *event*
  - Specification of what makes a *significant event*
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

[A642] Detect and Log Event

Description

In this activity, monitoring data from various system resources are input and converted into events. Monitoring data can be generated by a vast number of system resources. The data might be generated by a resource or by a monitor of that resource. This data is used to identify status changes to resources.

Many system resources generate monitoring data that is not indicative of a fault. This activity monitors that data in order to identify all potential events contained in the data. Events generated by this activity are also recorded. This information includes information about Managed Objects (MOs) related to events and might be necessary for the resolution of incidents, problems, reviewing SLAs, or other service management purpose.

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

Inputs

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.
- Security Monitoring Data (From: A72 A726)

  Information relating to the overall item-by-item outcomes from, and status of, security. This can include details of access requests, authentications processed, attacks received and warning thresholds triggered.
- 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.
- Identity and Access Monitoring Data (From: A67 A673 A674)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.
- Event Analysis Updates

  Any additional data added to (but not modifying) the primary data of a logged event as a result of other IT processes carrying out their investigations. Examples of such processes would be Incident, Capacity and Availability Management.
- Event_ Derived (From: A644)

  A new event created as a result of correlation across multiple events, usually signifying some new out-of-tolerance conditions requiring action.

Outputs

- Event (To: A643 A65 A654 A66 A662)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[41]

- Event Management Activity Data (To: A647)

  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 (of this process) feedback, priorities.

[A643] Filter Event

Description

The stream of logged events is examined and filtered to identify only those abnormal events for which a response is needed. These remaining events, designated as significant events, indicate an abnormal state of an MO. This set of significant events requires a response from either Event Management activities or from the Incident Management process. This activity is also responsible for determining the appropriate time frame for event resolution.

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

Inputs

- Event (From: A64 A642)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[42]

41. ITIL V3 Glossary
42. ITIL V3 Glossary

- Event_ Escalated (From: A644)

  An event, or set of events, that requires re-examination and filtering as a result of event processing or correlation. This is typically indicated by increasing the priority classification.

Outputs

- Event_ Significant (To: A644)

  Unsolicited, (formatted), significant information which must be communicated from a managed object for the purpose of meeting a management objective.

  An Alert is an example of a significant event. It is defined by ITIL as: “A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.”[43]

- Event Management Activity Data (To: A647)

  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 (of this process) feedback, priorities.

[A644] Correlate Events and Select Response

Description

This activity eliminates duplicate events, correlates multiple events, and throttles processing of repeated events. The criticality of the event is assessed to determine if it should be escalated.

Correlated events are either routed for handling within Incident Management or preferably, designated for automated resolution within the scope of Event Management. The Event Management Framework identifies rules used to determine how to process various categories of significant events. This can include opening an incident, changing the status or severity of an event, dropping an event, or sending the event for automated recovery (Resolve Events).

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

Inputs

- Event_ Significant (From: A643)

  Unsolicited, (formatted), significant information which must be communicated from a managed object for the purpose of meeting a management objective.

  An Alert is an example of a significant event. It is defined by ITIL as: “A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.”[44]

43. ITIL V3 Glossary

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.

- 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.

- Event_ Processed (To: A645)

  An event which has been analyzed for cause of out-of-tolerance conditions and led to its creation for which a plan, within the scope of Event Management, has been formulated to resolve those conditions.

- Event_ Ready for Closure (To: A646)

  The complete audit trail of an event and all states of processing through its life cycle.

- Event Management Activity Data (To: A647)

  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 (of this process) feedback, priorities.

- Event_ Derived (To: A642)

  A new event created as a result of correlation across multiple events, usually signifying some new out-of-tolerance conditions requiring action.

- Event_ Escalated (To: A643)

  An event, or set of events, that requires re-examination and filtering as a result of event processing or correlation. This is typically indicated by increasing the priority classification.

[A645] Resolve Event

Description

During this activity, events are flagged as ready for closure. Some events will have required no direct resolution action; others will have. In the latter case, this can mean that the fault has been corrected, and so closure is straightforward.

However, it can also be that the fault still exists and so an incident notification is needed. Depending upon the design of the Event Management solution, events of this type could be closed immediately or remain open until the relevant Service Management processes indicate readiness for closure.

In either case, when the event is closed the success or otherwise of its resolution is indicated.

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event

44. ITIL V3 Glossary

- Identification of significant events that can be processed (responded to), and what those procedures are
- Practices for logging and filtering events
- Definition of the event life cycle

Inputs

- Event_ Processed (From: A644)

  An event which has been analyzed for cause of out-of-tolerance conditions and led to its creation for which a plan, within the scope of Event Management, has been formulated to resolve those conditions.

Outputs

- Event Resolution Directive (To: A62 A622 A623 A624 A63 A634 A635)

  The set of commands or instructions to resource controlling activities which have been selected so that the event causing conditions will be resolved.
- 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
- Event_ Ready for Closure (To: A646)

  The complete audit trail of an event and all states of processing through its life cycle.
- Event Management Activity Data (To: A647)

  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 (of this process) feedback, priorities.

[A646] Close Event

Description

During this activity, events that went through Resolve Events are closed. Typically, this means that the fault has been corrected. However, it can also be that the fault still exists. In either case, the event is closed and the success of its resolution is indicated.

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

Inputs

- Event_ Ready for Closure (From: A644 A645)

  The complete audit trail of an event and all states of processing through its life cycle.
- Event Analysis Updates

  Any additional data added to (but not modifying) the primary data of a logged event as a result of other IT processes carrying out their investigations. Examples of such processes would be Incident, Capacity and Availability Management.

Outputs

- 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.
- Event_ Closed

  The event audit trail and life cycle with the addition of any information from the event closure activity.
- Event Management Activity Data (To: A647)

  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 (of this process) feedback, priorities.

[A647] Evaluate Event Management Performance

Description

Performance evaluation of the Event Management process aims to identify overall areas requiring improvement. For example, the foundation and interfaces of the process, all activities, their accomplishment, their degree of automation, as well as the roles and responsibilities including the respective skills. Basis for improvements are the insights and lessons learned from the observations and analysis of activity accomplishments and results.

In this activity, the performance of the Event Management process is analyzed and reported. The following are included in the analysis:

- Number and type of events
- Event trends
- Event resolution trends
- Event detection effectiveness
- Event filtering rules
- Event processing scripts
- Event management life cycle

Controls

- Event Management Framework (From: A641)

  Includes the following:

  - Specification of what makes an event
  - Specification of what makes a significant event
  - Identification of significant events that can be processed (responded to), and what those procedures are
  - Practices for logging and filtering events
  - Definition of the event life cycle

Inputs

- Event Management Activity Data (From: A642 A643 A644 A645 A646)

  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 (of this process) feedback, priorities.

Outputs

- Event Management Evaluation (To: A641)

  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.

[A65] Incident Management

Purpose

The purpose of the Incident Management process is to focus on the restoration of a service affected by any real or potential interruption which has impact upon the quality of that service.

Definition of incident: “An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example Failure of one disk from a mirror set.”[45]

Outcomes

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

- Following interruptions, IT service is rapidly restored
- IT service availability is sustained at a high level
- Workarounds to resolve similar service interruptions are created
- Potential improvements to services may be identified

Normal service operation is defined here as working within agreed service level targets.

Scope

The management of the life cycle of incidents (including reception, logging, acknowledgement, classification, response, tracking and reporting) for all components involved in the provision of IT service.

Includes

- Incidents reported by users or discovered within the IT organization by automation or people
- Handling (automatically or with human assistance) of system events that have been identified as incidents by the Event Management process
- Creation of workarounds
  - While service restoration has the highest priority, consideration has to be made of the risk that a workaround could exacerbate the original incident. For example, certain virus infections might spread beyond their initial scope if a simple service restoration is put into effect
- Implementation of workarounds (with Change Management, where required by the change policy)
- Participation within the procedures (typically involving several processes working in conjunction) defined for handling *major incidents*

45. ITIL V3 Glossary

Excludes

- Monitoring (Service Execution, Data Management)
- Responding to business-as-usual perturbations in the running of services (Event Management)
- Service requests (Request Fulfillment)
- IT Resilience – ensuring the continued readiness and integrity of the IT services (Resilience category processes)

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.

- 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.”[46]
  - 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.”[47]
  - 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.”[48]

  These agreements can be in a draft or finalized status.

- 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.

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

Inputs

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operational service. This can include measurements of resource utilization, transaction volumes, processing status, etc.

- 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 ore 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.

- Event (From: A64 A642)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[49]

- 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.

- 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.)

- 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.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

49. ITIL V3 Glossary

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

- 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.

- Incident_ Resolved (To: A62 A656 A657)

  An incident for which a workaround or fix has been successfully applied.

- Incident Information (To: A2 A24 A244 A61 A613 A615 A652 A653 A654 A655 A656 A66 A662 A7 A72 A726 A73 A736 A74 A744 A75 A754)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- Service Request (To: A61 A612)

  A request to perform a standard and straightforward IT task for a user. Service requests are tasks that are within the scope of existing IT services.

  ITIL definition: “A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted.”[50]

50. ITIL V3 Glossary

Activities

This process is composed of these activities:

- A651 Establish Incident Management Framework
- A652 Identify and Log Incident
- A653 Classify Incident and Provide Initial Support
- A654 Investigate and Diagnose Incident
- A655 Resolve Incident and Recover Service
- A656 Close Incident
- A657 Own, Monitor, Track and Communicate Incidents
- A658 Evaluate Incident Management Performance

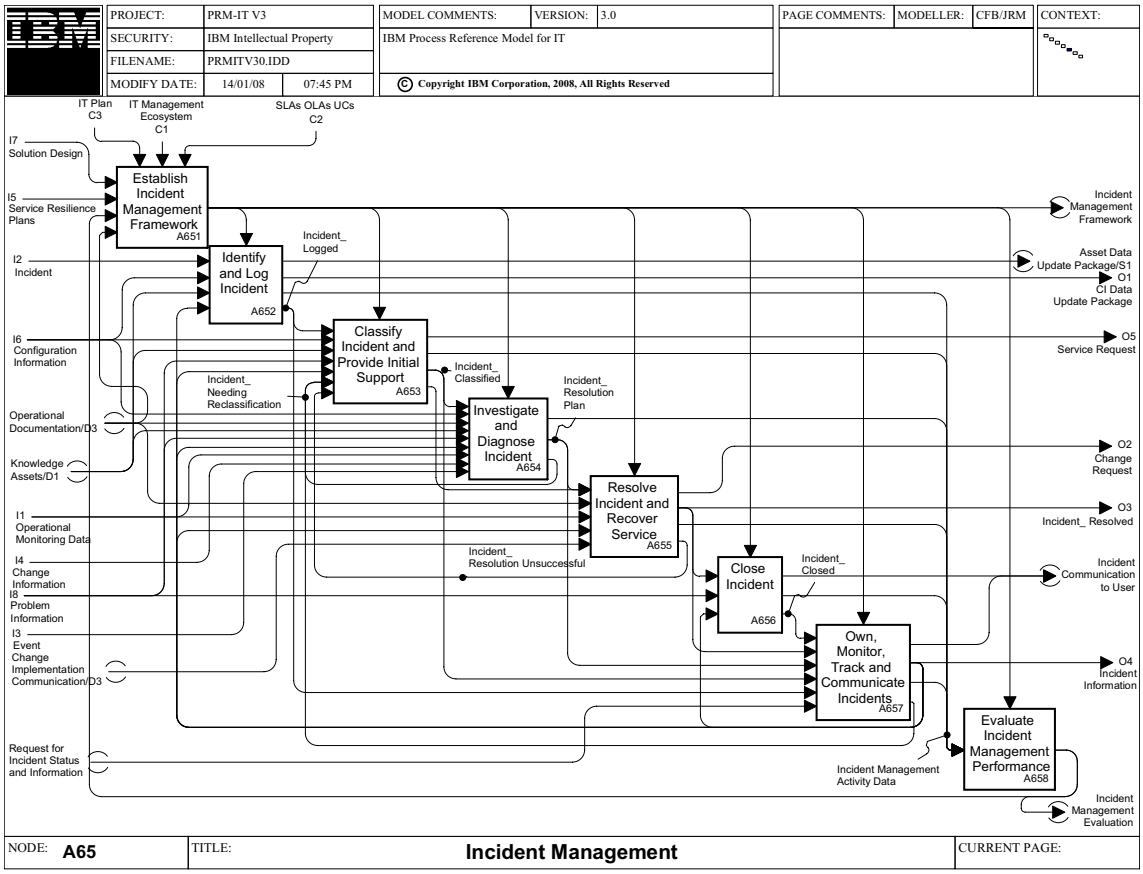

Figure 6. A65 Incident Management

[A651] Establish Incident Management Framework

Description

Define and maintain a framework of policies and procedures that guides and governs the behavior of the Incident 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 measurement and reporting of 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 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.
- 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.”[51]
  - 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.”[52]
  - 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

51. ITIL V3 Glossary
52. ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[53]

These agreements can be in a draft or finalized status.

Inputs

- 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.

- 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.)

- Incident Management Evaluation (From: A658)

  An analysis of how well the Incident Management process was performed. This can also include suggested areas for modifications to the Incident Management Framework.

- 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.

Outputs

- Incident Management Framework (To: A652 A653 A654 A655 A656 A657 A658)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

53. ITIL V3 Glossary

[A652] Identify and Log Incident

Description

To detect or acknowledge incidents from other activities, record basic details about the incident, notify Configuration Management and Asset Management processes as necessary. Also, to alert support groups as necessary.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- 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.
- 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.
- Knowledge Assets (From: A85 A855)

  Any information from knowledge management that fulfills a knowledge request.
- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

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.
- 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 Management Activity Data (To: A658)

  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.
- Incident_ Logged (To: A653 A657)

  An identified incident that has been saved in a database.

[A653] Classify Incident and Provide Initial Support

Description

Determine the impact, urgency and priority of logged incidents.

- Identify the reasons for the incident, using initial diagnosis
- Compare to Problems and Known Errors
- Correlate with other Incidents
- Assess related configuration details

If the incident is assessed as *no trouble found*, it is transferred to the Request Fulfillment process as a Service Request. Incidents exceeding a defined threshold of impact and urgency are categorized as Major Incidents and the appropriate procedure is invoked.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident_ Logged (From: A652)

  An identified incident that has been saved in a database.
- 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.
- Knowledge Assets (From: A85 A855)

  Any information from knowledge management that fulfills a knowledge request.
- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.
- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.
- Incident_ Needing Reclassification (From: A654 A657)

  An incident that requires to be moved to a different classification, perhaps to a different team.
- Incident_ Resolution Unsuccessful (From: A655)

  An incident for which a workaround or fix was not provided or was unsuccessful. Normally, an incident should eventually yield a workaround or a fix for that incident. However, in some situations, no workaround or fix works to resolve the incident.

Outputs

- Service Request (To: A61 A612)

  A request to perform a standard and straightforward IT task for a user. Service requests are tasks that are within the scope of existing IT services.

  ITIL definition: “A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted.”[54]

- Incident Management Activity Data (To: A658)

  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.

- Incident_ Classified (To: A654 A657)

  An incident that has been assigned a classification. The classification helps narrow the realm of possibilities for resolving the incident. For instance, the classification can be based on platform, type of problem, component, or other information.

- Incident_ Resolution Plan (To: A655 A657)

  An incident for which a resolution plan has been created or obtained. Subsequently (and beyond this activity), the resolution plan has to be applied and the outcome verified with the user.

[A654] Investigate and Diagnose Incident

Description

This activity assesses Incidents and all data associated with them in order to identify appropriate responses and actions, and to formulate Incident Resolution Plans.

Actions can include identifying workarounds, reclassifying the incident based on further analysis, and updating Incident records.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident_ Classified (From: A653)

  An incident that has been assigned a classification. The classification helps narrow the realm of possibilities for resolving the incident. For instance, the classification can be based on platform, type of problem, component, or other information.

- 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.

54. ITIL V3 Glossary

- 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.
- Knowledge Assets (From: A85 A855)

  Any information from knowledge management that fulfills a knowledge request.
- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.
- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.
- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.
- Change Information (From: A5 A51 A518)

  Covers the full scope of information about one or many changes, from individual detail within a particular change through ad hoc or pre-determined reporting of a set of changes.
- Event (From: A64 A642)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[55]

Outputs

- Incident Management Activity Data (To: A658)

  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.
- Incident_ Resolution Plan (To: A655 A657)

  An incident for which a resolution plan has been created or obtained. Subsequently (and beyond this activity), the resolution plan has to be applied and the outcome verified with the user.
- Incident Needing Reclassification (To: A653)

  An incident that requires to be moved to a different classification, perhaps to a different team.

55. ITIL V3 Glossary

[A655] Resolve Incident and Recover Service

Description

This activity takes actions necessary to resolve the incident and restore service using an existing solution work around or, alternatively, raising a change request (RFC) to effect a new solution.

It also prompts any action necessary to recover the service to committed levels of delivery.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident_ Resolution Plan (From: A653 A654)

  An incident for which a resolution plan has been created or obtained. Subsequently (and beyond this activity), the resolution plan has to be applied and the outcome verified with the user.

- 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.

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- 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.

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.

- Incident_ Resolved (To: A62 A656 A657)

  An incident for which a workaround or fix has been successfully applied.
- Incident Management Activity Data (To: A658)

  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.
- Incident_ Resolution Unsuccessful (To: A653)

  An incident for which a workaround or fix was not provided or was unsuccessful. Normally, an incident should eventually yield a workaround or a fix for that incident. However, in some situations, no workaround or fix works to resolve the incident.

[A656] Close Incident

Description

This activity examines the case history of an Incident which has reached *resolved* status. It ensures that all required incident documentation has been completed, including details of cause, resolution, outcome and effort expended. It reviews the original classification against whatever root cause information is available to determine the classification accuracy. In line with policy, it obtains stakeholder agreement with resolution activity and status.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:
  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident_ Resolved (From: A65 A655)

  An incident for which a workaround or fix has been successfully applied.
- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.
- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

Outputs

- Incident_ Communication to User

  Communications with a user about the status or progress of an incident. Could be to provide status information or to solicit additional data or request some user action as part of diagnosis.

- Incident Management Activity Data (To: A658)

  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.

- Incident_ Closed (To: A657)

  The finalization of all data related to an incident, including structured data which supports analysis of incident causes, patterns, costs and resolution effectiveness.

[A657] Own, Monitor, Track and Communicate Incidents

Description

This activity ensures that the Incident is managed throughout its entire life cycle. It examines the data and status changes (noted in other activities within the Incident Management process) as recorded in Incident Records, defined in ITIL as: “A Record containing the details of an Incident. Each Incident record documents the Life cycle of a single Incident.”[56]

Aspects of the activity include:

- Monitoring status and incident impact on service level agreements
- Incident reclassification and escalation if necessary
- Maintaining incident information
- Communicating status and progress to stakeholders and support groups

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident_ Closed (From: A656)

  The finalization of all data related to an incident, including structured data which supports analysis of incident causes, patterns, costs and resolution effectiveness.

- Incident_ Resolved (From: A65 A655)

  An incident for which a workaround or fix has been successfully applied.

- Incident_ Resolution Plan (From: A653 A654)

  An incident for which a resolution plan has been created or obtained. Subsequently (and beyond this activity), the resolution plan has to be applied and the outcome verified with the user.

- Incident_ Classified (From: A653)

  An incident that has been assigned a classification. The classification helps narrow the realm of possibilities for resolving the incident. For instance, the classification can be based on platform, type of problem, component, or other information.

- Incident_ Logged (From: A652)

  An identified incident that has been saved in a database.

56. ITIL V3 Glossary

- Request for Incident Status and Information

  Notification of the need for information about incidents.

Outputs

- Incident_ Communication to User

  Communications with a user about the status or progress of an incident. Could be to provide status information or to solicit additional data or request some user action as part of diagnosis.
- Incident Information (To: A2 A24 A244 A61 A613 A615 A652 A653 A654 A655 A656 A66 A662 A7 A72 A726 A73 A736 A74 A744 A75 A754)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.
- Incident Management Activity Data (To: A658)

  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.
- Incident_ Needing Reclassification (To: A653)

  An incident that requires to be moved to a different classification, perhaps to a different team.

[A658] Evaluate Incident Management Performance

Description

The purpose of this activity is to evaluate the performance of the Incident Management process activities against defined performance criteria and measures, and to provide input to the IT Management System framework.

Controls

- Incident Management Framework (From: A651)

  The set of policies and procedures for performing the Incident Management process, including data items such as:

  - Priority and severity classification schemes
  - Resolution targets
  - Tables identifying teams to be assigned, by system or service

Inputs

- Incident Management Activity Data (From: A652 A653 A654 A655 A656 A657)

  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

- Incident Management Evaluation (To: A651)

  An analysis of how well the Incident Management process was performed. This can also include suggested areas for modifications to the Incident Management Framework.

[A66] Problem Management

Purpose

The purpose of the Problem Management process is to resolve problems affecting the IT service, both reactively and proactively. Problem Management finds trends in incidents, groups those incidents into problems, identifies the root causes of problems, and initiates change requests (RFCs) against those problems.

Definition of problem: “A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management Process is responsible for further investigation.”[57]

Outcomes

As a result of the successful implementation of this process:

- The number and adverse impact of incidents and problems is minimized
- Potential incidents are prevented
- Recurrence of incidents is prevented
- The management of incidents is more effective and efficient
- The productivity of support staff is improved

  For example, by improving Service Desk first time fix rate

An effective problem management process maximizes system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.

Scope

The process is primarily concerned with establishing the root cause of an incident and its subsequent resolution and prevention. The reactive function is to solve problems relating to one or more incidents. The proactive function is to identify and solve problems before incidents occur.

Effective problem management requires the identification and classification of problems, root cause analysis, and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records, and review of the status of corrective actions.

Includes

- Root cause analysis and identification
- Solution (and workaround) definition and selection
- Submission of change requests (RFCs)
- Appropriate prioritization of resources required for resolution based on business need
- Contribution to the collective problem resolution knowledge base

Excludes

- Identification, creation and resolution of incidents (Incident Management)

57. ITIL V3 Glossary

- Actual implementation of the resolution of a problem. Problem Management initiates their resolution through Change Management and participates in the Post Implementation Review (PIR)
- Knowledge management methodology (Knowledge Management)

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.

- 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.”[58]
  - 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.”[59]
  - 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.”[60]

  These agreements can be in a draft or finalized status.

- 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 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.

58. ITIL V3 Glossary
59. ITIL V3 Glossary
60. ITIL V3 Glossary

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.”[61]

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- Event (From: A64 A642)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[62]

- 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.

- 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.)

- 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.

61. ITIL V3 Glossary
62. ITIL V3 Glossary

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.

- Problem Information (To: A2 A24 A244 A245 A356 A61 A613 A615 A65 A653 A654 A656 A662 A663 A664 A665 A666 A7 A73 A736 A74 A744 A76 A764)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

Activities

This process is composed of these activities:

- A661 Establish Problem Management Framework
- A662 Detect and Log Problem
- A663 Categorize and Prioritize Problem
- A664 Investigate and Diagnose Problem
- A665 Resolve Problem
- A666 Close and Review Problem
- A667 Monitor, Track and Report Problems
- A668 Evaluate Problem Management Performance

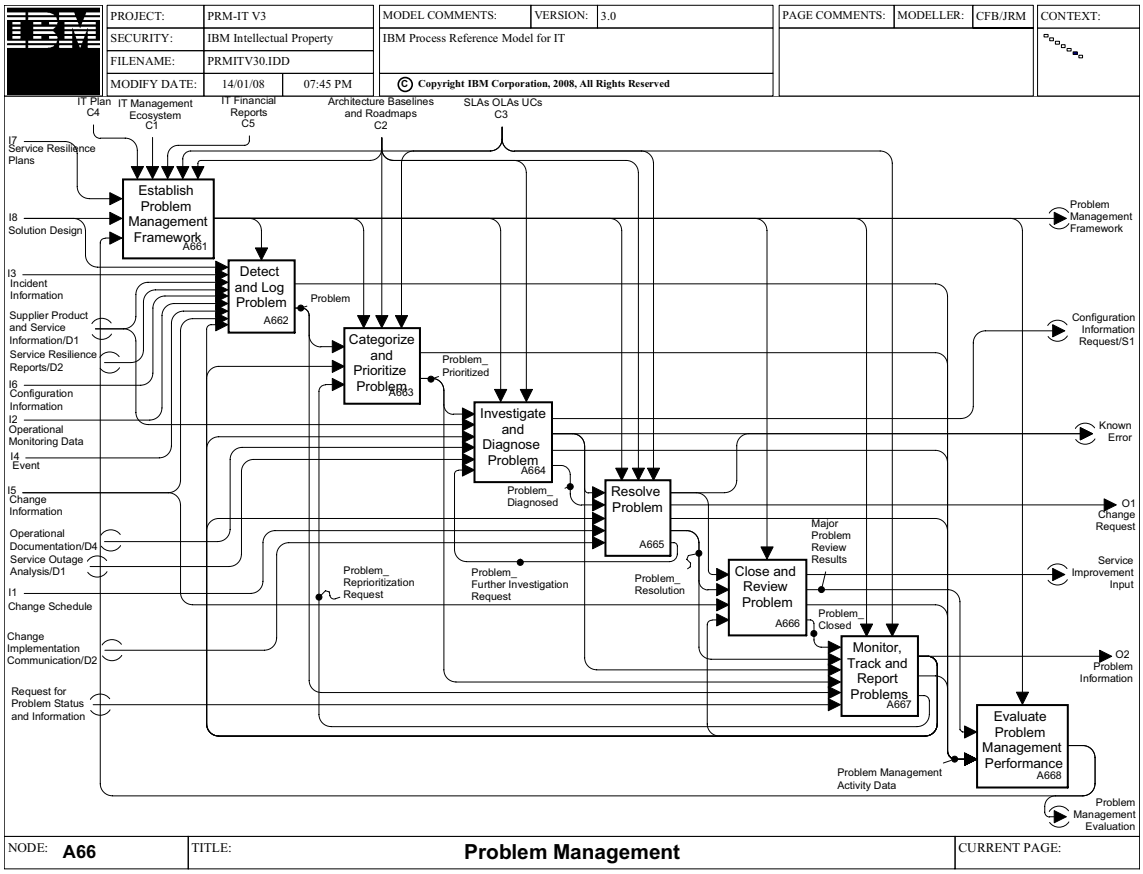

Figure 7. A66 Problem Management

[A661] Establish Problem Management Framework

Description

This activity identifies resources necessary for the total process to function as desired and designed. It is within this activity that:

- Interfaces and relationships to other processes are identified
- Information inputs and outputs are identified
- Guidelines for problem classification and prioritization are defined
- Sources and receivers of information necessary for Problem Management to be effective are identified
- Tool requirements are documented
- Successful process measurement criteria are documented
- Roles and responsibilities (including the role of the process owner) must be tailored to meet the requirements of the organization and must be assigned
- Skill requirements are identified and training is requested if needed

Service levels with regard to Problem Management have to be taken into account during this activity. Finally, the structure and process of Problem Management have to be communicated to those concerned.

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.

- 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.

- 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.”[63]

63. ITIL V3 Glossary

- 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.

- 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

- 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.

- Problem Management Evaluation (From: A668)

  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

- Problem Management Framework (To: A662 A663 A664 A665 A666 A667 A668)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

64. ITIL V3 Glossary
65. ITIL V3 Glossary

[A662] Detect and Log Problem

Description

Whether it is for proactive problem handling or reactive problem activities, this activity ensures that monitoring, analysis, and notification mechanisms are implemented to detect problems. Once detected, problems are fully recorded and linked to the associated incidents. Incidents provide the primary source for problem detection; the activity includes further ways to identify problems:

- Notification from suppliers
- Feedback from the service desk or technical support groups
- Proactive approaches like trend analysis.

Problem detection and logging can include both automated and manual activities. The result of this activity is the formal creation of a problem, with the relevant details captured in a problem record.

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

Inputs

- 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.

- Incident Information (From: A6 A65 A657)

  Information about one or more incidents. Can range from full details of an individual incident through collated and summarized information about sets of incidents.

- Supplier Product and Service Information (From: A826)

  Information about the items (products or services) that can be supplied by the suppliers in the portfolio, like the catalog of orderable supply items, including:

  - Prices
  - Service levels
  - Supply options (suppliers can provide supply items)

  Covers both external and internal suppliers. An example of an internal supplier: Facility supplier indicates lead-time and costs for equipping a new workspace.

- Service Resilience Reports

  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.)

These reports detail the volumes, attainments, issues outstanding and other characteristics detailing the performance and contribution to the overall delivery of service. They include efficiency reviews and audit reports.

- 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.

- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)

  Information relating to the overall item-by-item outcomes and status of the IT operation service. This can include measurements of resource utilization, transaction volumes, processing status, among others.

- Event (From: A64 A642)

  Details of individual and collective events. They are available to any Service Management process for investigation, diagnosis and other analytical purposes on a real-time or historical basis.

  ITIL defines Alert as: “A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.”[66]

- 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.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

Outputs

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that support the evaluation of the overall Problem Management process.

- Problem (To: A663 A667)

  As defined in ITIL: “A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.”[67]

66. ITIL V3 Glossary
67. ITIL V3 Glossary

[A663] Categorize and Prioritize Problem

Description

This activity ensures that problems are classified to enable appropriate analysis and resolution. It further takes into account the severity of problems that can be encountered, and the potential impact to business goals. The result of this activity is a prioritized problem.

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

- 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.

- 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.”[68]
  - 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.”[69]
  - 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.”[70]

  These agreements can be in a draft or finalized status.

Inputs

- Problem (From: A662)

  As defined in ITIL: “A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.”[71]

68. ITIL V3 Glossary
69. ITIL V3 Glossary
70. ITIL V3 Glossary

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

- Problem_ Reprioritization Request (From: A667)

  In the course of monitoring and tracking problems there could be a need to lower or raise the priority of an individual problem due to a change in the business impact. The problem is referred for reprioritization.

Outputs

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that support the evaluation of the overall Problem Management process.

- Problem_ Prioritized (To: A664 A667)

  A problem for which the category and priority are understood and recorded in the problem record. ITIL has the following definitions for these terms:

  - Category is defined as "A named group of things that have something in common."[72]
  - Priority is defined as "A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken."[73]

[A664] Investigate and Diagnose Problem

Description

Investigate and Diagnose Problem includes activities for *root cause analysis*, creating workarounds where possible, and recording a known error. This activity must ensure that workarounds are in place and effective, and that sufficient analysis and diagnosis has ensued to complete the root cause analysis. The result of this activity will be:

- The creation of a *known error record* that describes the diagnosis and available workarounds
- An updated problem record that indicates the diagnosed problem

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

- 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.

71. ITIL V3 Glossary
72. ITIL V3 Glossary
73. ITIL V3 Glossary

Inputs

- Problem_ Prioritized (From: A663)

  A problem for which the category and priority are understood and recorded in the problem record. ITIL has the following definitions for these terms:

  - Category is defined as “A named group of things that have something in common.”[74]
  - Priority is defined as “A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken.”[75]

- Supplier Product and Service Information (From: A826)

  Information about the items (products, services) that can be supplied by the suppliers in the portfolio, like the catalog of orderable supply items including

  - Prices
  - Service levels
  - Supply options, (suppliers can provide these supply items)

  Covers both external and internal suppliers. An example of an internal supplier: Facility supplier indicates lead-time and costs for equipping a new workspace.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

- 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.

- Service Outage Analysis (From: A736)

  The results from identifying root causes of service outage, assessing the effectiveness of service availability, and identifying key recommendations for improving availability. There is a corresponding technique described in the ITIL *Service Delivery*, Availability Management book.

- Problem_ Further Investigation Request (From: A665)

  In the process of resolving a known error, if additional problems are identified, a request is made for additional root cause analysis.

Outputs

- Configuration Information Request (To: A54 A544)

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

- Known Error (To: A665 A666 A667)

  As defined in ITIL: “A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Life cycle by Problem Management. Known Errors may also be identified by Development or Suppliers.”[76]

74. ITIL V3 Glossary
75. ITIL V3 Glossary
76. ITIL V3 Glossary

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that support the evaluation of the overall Problem Management process.

- Problem_ Diagnosed (To: A665)

  A problem for which the root cause is understood.

[A665] Resolve Problem

Description

This activity ensures the resolution of known errors (that is, problems for which the root cause is fully understood). This includes the search for a solution, the implementation planning of resolution actions to eliminate known errors (initiating an RFC or a Project Proposal), and tracking the successful implementation of the change to the infrastructure. The submission of an RFC or Project Proposal is a result of this activity. The error resolution has to be documented in the problem and known error records.

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

- 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.

- 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.”[77]
  - 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.”[78]
  - 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

77. ITIL V3 Glossary
78. ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[79]

These agreements can be in a draft or finalized status.

Inputs

- Known Error (From: A664 A665)

  As defined in ITIL: "A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Life cycle by Problem Management. Known Errors may also be identified by Development or Suppliers."[80]

- Problem_ Diagnosed (From: A664)

  A problem for which the root cause is understood.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

- 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."[81]

- 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.

Outputs

- Known Error (To: A665 A666 A667)

  As defined in ITIL: "A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Life cycle by Problem Management. Known Errors may also be identified by Development or Suppliers."[82]

- 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.

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that supports the evaluation of the overall Problem Management process.

79. ITIL V3 Glossary
80. ITIL V3 Glossary
81. ITIL V3 Glossary
82. ITIL V3 Glossary

- Problem_ Resolution (To: A666 A667)

  Actions taken to repair permanently a known error or implement a workaround.

- Problem_ Further Investigation Request (To: A664)

  In the process of resolving a known error, if additional problems are identified, a request is made for additional root cause analysis.

[A666] Close and Review Problem

Description

This activity includes closing problems, ensuring that known error records have been updated, and performing reviews for major problems. Each problem record is checked for completeness so that other processes have the appropriate information available.

- For example, incident management could need to close or update incidents as a result of the problem resolution and closure.

For each major problem, a review will be conducted and the results incorporated in communication, training, and reviewing the service.

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

Inputs

- Known Error (From: A664 A665)

  As defined in ITIL: “A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Life cycle by Problem Management. Known Errors may also be identified by Development or Suppliers.”[83]

- Problem_ Resolution (From: A665)

  Actions taken to repair permanently a known error or implement a workaround.

- 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.

- Problem Information (From: A6 A66 A667)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

Outputs

- Service Improvement Input

  Any information from problem resolution (proactively or reactively) that can help to improve the overall service delivery. For example, there could be a finding that a specific service part or component frequently generates problems and a determination that a modification

83. ITIL V3 Glossary

to the procedures used to operate the service would remove the incident-inducing circumstances.

- Major Problem Review Results (To: A668)

  The analysis and outcome of reviewing those problems classified as major. This classification can reflect a variety of reasons, such as:

  - Service impact
  - Problem duration
  - Cost and efficiency to achieve resolution and closure

  Review outputs will reflect these topics.

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that supports the evaluation of the overall Problem Management process.

- Problem_ Closed (To: A667)

  The finalization of all data related to a problem. This includes structured data, which supports analysis of problem causes, patterns, costs and resolution effectiveness.

[A667] Monitor, Track and Report Problems

Description

This activity is responsible for examining all information about all problems, using the records updated by the other activities within the Problem Management process. ITIL defines a Problem Record as “A Record containing the details of a Problem. Each Problem Record documents the Life cycle of a single Problem.”[84]

The ongoing monitoring and tracking of the handling of problems and known errors must be accomplished to report on service level attainment with regard to problem management. The reports and relevant statistics are created mainly based on problem record data. It could also take into account feedback from customers.

This monitoring and reporting activity has to be done regularly, but can also be initiated by a special request. It might result in problems being reprioritized and might prompt further *root cause analysis* and the development of new resolution plans. An additional result of this activity is problem information that is used in service reviews.

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

- 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.

84. 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.”[85]
- 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.”[86]
- 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.”[87]

These agreements can be in a draft or finalized status.

Inputs

- Problem_ Closed (From: A666)

  The finalization of all data related to a problem. This includes structured data, which supports analysis of problem causes, patterns, costs and resolution effectiveness.
- Problem_ Resolution (From: A665)

  Actions taken to repair permanently a known error or implement a workaround.
- Known Error (From: A664 A665)

  As defined in ITIL: “A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Life cycle by Problem Management. Known Errors may also be identified by Development or Suppliers.”[88]
- Problem_ Prioritized (From: A663)

  A problem for which the category and priority are understood and recorded in the problem record. ITIL has the following definitions for these terms:

  - Category is defined as “A named group of things that have something in common.”[89]
  - Priority is defined as “A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken.”[90]
- Problem (From: A662)

  As defined in ITIL: “A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.”[91]
- Request for Problem Status and Information

  Request for information with regard to overall problem status and service level attainment with regard to problem management.

85. ITIL V3 Glossary
86. ITIL V3 Glossary
87. ITIL V3 Glossary
88. ITIL V3 Glossary
89. ITIL V3 Glossary
90. ITIL V3 Glossary
91. ITIL V3 Glossary

Outputs

- Problem Information (To: A2 A24 A244 A245 A356 A61 A613 A615 A65 A653 A654 A656 A662 A663 A664 A665 A666 A7 A73 A736 A74 A744 A76 A764)

  Information about one or more problems. Can range from full details of an individual problem through to collated and summarized information about sets of problems. Can be provided both as formal reports (such as documents to customers describing root cause, contributing factors and corrective actions) and informally as structured data for other processes to analyze for their own purposes.

- Problem Management Activity Data (To: A668)

  Any data about the accomplishment of process activities that supports the evaluation of the overall Problem Management process.

- Problem_ Reprioritization Request (To: A663)

  In the course of monitoring and tracking problems, there could be a need to lower or raise the priority of an individual problem due to a change in the business impact. The problem is referred to reprioritization.

[A668] Evaluate Problem Management Performance

Description

This activity is responsible for the ongoing assessment and management of the Problem Management process, according to predetermined criteria. It is responsible for managing and reporting process measurements at regularly scheduled intervals. Also, the generation of any improvement opportunity areas that might be necessary to facilitate meeting business objectives.

Basis for the improvements are insights and lessons learned from the observations and analysis of activity accomplishments and results.

Basically, the improvements should lead to more efficiency in the process (better Problem Management).

Controls

- Problem Management Framework (From: A661)

  The framework that contains all relevant information about the structure of the Problem Management process; that is, the strategic goals and policies for Problem Management, the definition of supporting technology, measurements, among others.

Inputs

- Major Problem Review Results (From: A666)

  The analysis and outcome of reviewing those problems classified as major. This classification can reflect a variety of reasons, such as:

  - Service impact
  - Problem duration
  - Cost and efficiency to achieve resolution and closure

  Review outputs will reflect these topics.
- Problem Management Activity Data (From: A662 A663 A664 A665 A666 A667)

  Any data about the accomplishment of process activities that supports the evaluation of the overall Problem Management process.

Outputs

- Problem Management Evaluation (To: A661)

  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.

[A67] Identity and Access Management

Purpose

The purpose of the Identity and Access Management process is to establish and maintain a registry of IT user identities and their associated access rights for each service. The registry provides a key reference for the authorization or rejection by the Security Management process of service usage attempts.

The process provides the ability to control and track who has access to data and services. It contributes to achieving the appropriate confidentiality, availability, and integrity of the organization's data.

ITIL definition of identity: "A unique name that is used to identify a user, person or role. The identity is used to grant rights to that user, person, or role."[92] This definition is narrower than those established in ISO standards relating to security. For the purposes of this process, the user might not be directly linked to one or more persons; it can take the form of an IT product or system for which access rights must be established and tracked, and for which an identity is therefore established.[93]

Definition of rights: "Entitlements, or permissions, granted to a user or role. For example, the right to modify particular data, or to authorize a change."[94]

Outcomes

As a result of the successful implementation of the Identity and Access Management process:

- An accurate and complete identity registry and associated rights is maintained
- There is a definitive source so that decisions can be made allowing users have access to information and the services they need while unauthorized access attempts are denied
- Authorized access to data and services is aligned with security policies
- Records of access attempts can be audited
- The data necessary to demonstrate compliance in relation to service and information access is available

Scope

This process operates within the set of controls described by the IT Security Policy, which itself takes direction from the Business Security Policy. The users for whom (or which) an identity is registered include not only those outside the IT organizational entity but also all resources involved in running the IT capability itself. Levels of control of identities and access rights will vary depending upon the scope of access required and the level of potential harm (fraud) from malicious access.

Access policies can be dynamic, reflecting the need to vary access rights depending on the time of day or the role being performed. The process must recognize that the authority to give access rights, or even to delegate the authority to give access rights, is a normal activity for many users.

Includes

- An identity schema aligned with business and security policies

92. ITIL V3 Glossary
93. ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security*. "Part 1: Introduction and general model." Widely known as the *Common Criteria*.
94. ITIL V3 Glossary

- Establishment and maintenance of identities
- Establishment and maintenance of access rights
- Translation of business rules for roles and group authorities so as to enact then within the identity schema
- Access to the registry for those processes providing affiliated security services, like physical access (Facilities Management)
- Raising warnings or revoking access rights when access attempt thresholds are breached

Excludes

- Definition, implementation, and operation of authentication mechanisms (Security Management)
- Enforcement of access rights (Security Management)
- Definition of the rules for business role and group authorities – defined by the business
- Physical security and access (Facilities Management)
- Security policies – defined by the business and 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.

- 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.”[95]

- 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.”[96]
- 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.”[97]

These agreements can be in a draft or finalized status.

- 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.
- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered *secure*. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- Identity and Access Work Request (From: A535 A62 A624)

  An identity and access request originating from another process.
- 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 Monitoring Data (From: A72 A726)

  Information relating to the overall item-by-item outcomes from, and status of, security. This can include details of access requests, authentications processed, attacks received and warning thresholds triggered.
- 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.
- Security Directives (From: A725)

  The directive to take action, or the action to be taken, so that the protections which implement the desired security practices are properly operated.
- Security Plan (From: A72 A725)

  A consolidated view and documentation of the resources, approach, procedures and assets to be protected together with a definition of the security practices and controls which will be enacted in order to fulfill the security policy. It covers both technical capabilities (for example, firewalls, encryption) and non-technical considerations (such as segregation of duties, training needs, user responsibilities).

95. ITIL V3 Glossary
96. ITIL V3 Glossary
97. 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.

Outputs

- Identity and Access Rights Register (To: A674 A675 A7 A72 A726 A727 A75 A754)

  The records which provide the current (and perhaps historical) values for identities and for access rights. This collective register is generated by actions related to identity life cycle management (enrollment, provisioning and user self-care), identity controls (access and privacy controls, single sign-on), identity federation (sharing user authentication and attribute information between trusted Web services applications), and identity foundation services (directory and workflow).

- Identity and Access Monitoring Data (To: A64 A642 A675 A727)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.

- 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 ore 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.

Activities

This process is composed of these activities:

- A671 Establish Identity and Access Management Framework
- A672 Evaluate and Verify Identity and Access Request
- A673 Create and Maintain Identity
- A674 Provide and Maintain Access Rights
- A675 Monitor and Report Identity and Access
- A676 Evaluate Identity and Access Management Performance

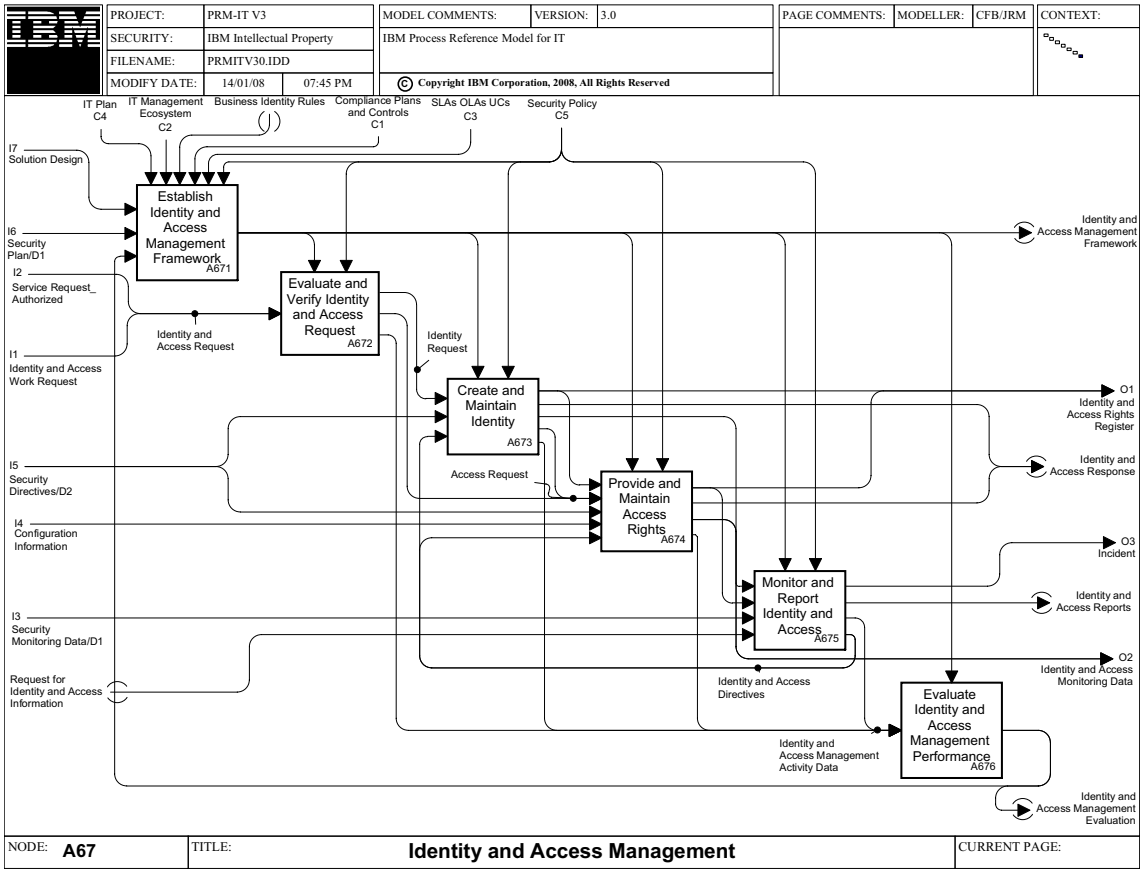

Figure 8. A67 Identity and Access Management

[A671] Establish Identity and Access Management Framework

Description

This activity defines a framework of policies, procedures, organizational roles and responsibilities, and other information under which the Identity and Access Management process will operate to meet its mission and goals. It is within this activity that:

- Interfaces and relationships to other processes are identified
- Information inputs and outputs are identified
- Sources and receivers of information necessary for Identity and Access Management to be effective are identified
- Tool requirements are documented
- Successful process measurement criteria are documented
- Roles and responsibilities (including the role of the process owner) must be tailored to meet the requirements of the organization and must be assigned
- Skill requirements are identified and training is requested if needed

Service levels with regard to Identity and Access Management have to be taken into account during this activity. Finally, the structure and process of Identity and Access Management have to be communicated to those concerned.

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.

- Business Identity Rules

  Set of rules that will be used to determine if identity requests and access requests will be approved. Part of Business Security Policies and Plans.

- 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.”[98]
  - 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.”[99]
  - 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.”[100]

  These agreements can be in a draft or finalized status.

98. ITIL V3 Glossary
99. ITIL V3 Glossary
100. ITIL V3 Glossary

- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered secure. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- 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.

- Security Plan (From: A72 A725)

  A consolidated view and documentation of the resources, approach, procedures and assets to be protected together with a definition of the security practices and controls which will be enacted in order to fulfill the security policy. It covers both technical capabilities (for example, firewalls, encryption) and non-technical considerations (such as segregation of duties, training needs, user responsibilities).

- Identity and Access Management Evaluation (From: A676)

  An assessment of the overall performance of the process and of its activities against the targets set in the Identity and Access Management process framework. It includes identification of potential process improvement items. This may also include proposed modifications to the Identity and Access Management Framework.

Outputs

- Identity and Access Management Framework (To: A672 A673 A674 A675 A676)

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

[A672] Evaluate and Verify Identity and Access Request

Description

This activity evaluates and verifies the identity of the person listed in each request and verifies that a reasonable substantiation is provided for the access to a system or application. This activity also verifies that the request has been approved by a legitimate approver.

Controls

- Identity and Access Management Framework (From: A671)

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

- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered secure. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- Identity and Access Request

  Service Request to create or modify an identity record for a user and to provide access to systems, data and applications.

Outputs

- Identity Request (To: A673)

  A form of Service Request to enroll, provision or change a given user's identity characteristics and which evaluated, verified and accepted for processing.
- Access Request (To: A674)

  An access request that has been evaluated and verified. Each access request is associated with a verified user identity.
- Identity and Access Management Activity Data (To: A676)

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

[A673] Create and Maintain Identity

Description

This activity will create new identity records in the identity database and will perform edits and deletes to existing identity records.

Controls

- Identity and Access Management Framework (From: A671)

  The policies, guidelines, plans, procedures, organizational roles and responsibilities and other information under which the Identity and Access Management process will operate to meet its mission and goals.
- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered secure. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- Identity Request (From: A672)

  A form of Service Request to enroll, provision or change a given user's identity characteristics and which evaluated, verified and accepted for processing.
- Security Directives (From: A725)

  The directive to take action, or the action to be taken, so that the protections which implement the desired security practices are properly operated.
- Identity and Access Directives (From: A675)

  Individual or collective commands, instructions or other requests to modify or adjust identities or the access rights register. Such directives are usually the result of monitoring patterns of identity and access behavior as well as from security monitoring data.

Outputs

- Identity and Access Rights Register (To: A674 A675 A7 A72 A726 A727 A75 A754)

  The records which provide the current (and perhaps historical) values for identities and for access rights. This collective register is generated by actions related to identity life cycle management (enrollment, provisioning and user self-care), identity controls (access and privacy controls, single sign-on), identity federation (sharing user authentication and attribute information between trusted Web services applications), and identity foundation services (directory and workflow).

- Identity and Access Response (To: A535 A624)

  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.

- Identity and Access Monitoring Data (To: A64 A642 A675 A727)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.

- Access Request (To: A674)

  An access request that has been evaluated and verified. Each access request is associated with a verified user identity.

- Identity and Access Management Activity Data (To: A676)

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

[A674] Provide and Maintain Access Rights

Description

This activity provides the access rights based on predefined policies and regulations. It updates the identity records to reflect the updated access rights and confirms that the access rights have been implemented.

Access rights can be removed as well as granted. Accordingly, this activity will restrict or revoke rights in order to execute policies and decisions made by appropriate authorities.

Controls

- Identity and Access Management Framework (From: A671)

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

- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered secure. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- Identity and Access Rights Register (From: A6 A67 A673 A674)

  The records which provide the current (and perhaps historical) values for identities and for access rights. This collective register is generated by actions related to identity life cycle management (enrollment, provisioning and user self-care), identity controls (access and privacy controls, single sign-on), identity federation (sharing user authentication and attribute information between trusted Web services applications), and identity foundation services (directory and workflow).

- Access Request (From: A672 A673)

  An access request that has been evaluated and verified. Each access request is associated with a verified user identity.

- Security Directives (From: A725)

  The directive to take action, or the action to be taken, so that the protections which implement the desired security practices are properly operated.

- 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.

- Identity and Access Directives (From: A675)

  Individual or collective commands, instructions or other requests to modify or adjust identities or the access rights register. Such directives are usually the result of monitoring patterns of identity and access behavior as well as from security monitoring data.

Outputs

- Identity and Access Rights Register (To: A674 A675 A7 A72 A726 A727 A75 A754)

  The records which provide the current (and perhaps historical) values for identities and for access rights. This collective register is generated by actions related to identity life cycle management (enrollment, provisioning and user self-care), identity controls (access and privacy controls, single sign-on), identity federation (sharing user authentication and attribute information between trusted Web services applications), and identity foundation services (directory and workflow).

- Identity and Access Response (To: A535 A624)

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

  - For an identiy 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

- Identity and Access Monitoring Data (To: A64 A642 A675 A727)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.

- Identity and Access Management Activity Data (To: A676)

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

[A675] Monitor and Report Identity and Access

Description

This activity includes logging, tracking and auditing access to systems and applications. This activity also includes the recurring validation of identity records for currency. Finally, this activity will produce regular and ad hoc reports.

Controls

- Identity and Access Management Framework (From: A671)

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

- Security Policy (From: A7 A72 A722)

  The statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered secure. It provides management direction into the allowable behaviors of the actors working with the resources and exercising the capabilities. It defines the scope of management and specifies the requirements for the security controls.

Inputs

- Identity and Access Monitoring Data (From: A67 A673 A674)

  Data produced during or about the processing performed against identities and access right records. In addition to item-by-item outcomes, the data can include measurements of resource utilization, transaction volumes, processing status, among others.

- Identity and Access Rights Register (From: A6 A67 A673 A674)

  The records which provide the current (and perhaps historical) values for identities and for access rights. This collective register is generated by actions related to identity life cycle management (enrollment, provisioning and user self-care), identity controls (access and privacy controls, single sign-on), identity federation (sharing user authentication and attribute information between trusted Web services applications), and identity foundation services (directory and workflow).

- Security Monitoring Data (From: A72 A726)

  Information relating to the overall item-by-item outcomes from, and status of, security. This can include details of access requests, authentications processed, attacks received and warning thresholds triggered.

- Request for Identity and Access Information

  A request from another process or from a customer or user for information on some aspect of one or more identities and their registered access rights, including historical data.

Outputs

- 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.

- Identity and Access Reports

  These reports contain a summary of identity and access records, and the amount and type of identity and access transaction completed (additions, changes, deletions) in a given timeframe.

- Identity and Access Management Activity Data (To: A676)

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

- Identity and Access Directives (To: A673 A674)

  Individual or collective commands, instructions or other requests to modify or adjust identities or the access rights register. Such directives are usually the result of monitoring patterns of identity and access behavior as well as from security monitoring data.

[A676] Evaluate Identity and Access Management Performance

Description

This activity assesses the performance of the Identity and Access Management activities against defined performance criteria and measures. 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

- Identity and Access Management Framework (From: A671)

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

Inputs

- Identity and Access Management Activity Data (From: A672 A673 A674 A675)

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

Outputs

- Identity and Access Management Evaluation (To: A671)

  An assessment of the overall performance of the process and of its activities against the targets set in the Identity and Access Management process framework. It includes identification of potential process improvement items. This may also include proposed modifications to the Identity and Access Management Framework.

PRM-IT A6 Node Tree

A6 – OPERATIONS	
A61	**Request Fulfillment**
A611	Establish Request Fulfillment Framework
A612	Receive and Approve Service Request
A613	Fulfill or Route Service Request
A614	Close Service Request
A615	Own, Monitor, Track and Communicate Service Requests
A616	Evaluate Request Fulfillment Performance
A62	**Service Execution**
A621	Establish Service Execution Framework
A622	Schedule and Adjust Workload
A623	Assign and Control Delivery Resources
A624	Deliver Service
A625	Monitor and Report Service Execution Operations
A626	Evaluate Service Execution Performance
A63	**Data Management**
A631	Establish Data Management Framework
A632	Plan Data Portfolio Lifecycle
A633	Acquire and Prepare Data
A634	Control, Deploy and Maintain Data
A635	Backup and Restore Data
A636	Dispose of Data
A637	Monitor and Report Data Management Operations
A638	Evaluate Data Management Performance
A64	**Event Management**
A641	Establish Event Management Framework
A642	Detect and Log Event
A643	Filter Event
A644	Correlate Events and Select Response
A645	Resolve Event
A646	Close Event
A647	Evaluate Event Management Performance
A65	**Incident Management**
A651	Establish Incident Management Framework
A652	Identify and Log Incident
A653	Classify Incident and Provide Initial Support
A654	Investigate and Diagnose Incident
A655	Resolve Incident and Recover Service
A656	Close Incident
A657	Own, Monitor, Track and Communicate Incidents
A658	Evaluate Incident Management Performance

A6 – OPERATIONS	
A66	**Problem Management**
A661	Establish Problem Management Framework
A662	Detect and Log Problem
A663	Categorize and Prioritize Problem
A664	Investigate and Diagnose Problem
A665	Resolve Problem
A666	Close and Review Problem
A667	Monitor, Track and Report Problems
A668	Evaluate Problem Management Performance
A67	**Identity and Access Management**
A671	Establish Identity and Access Management Framework
A672	Evaluate and Verify Identity and Access Request
A673	Creae and Maintain Identity
A674	Provide and Maintain Access Rights
A675	Monitor and Report Identity and Access
A676	Evaluate Identity and Access Management Performance

Figure 9. A6 Operations Node Tree

