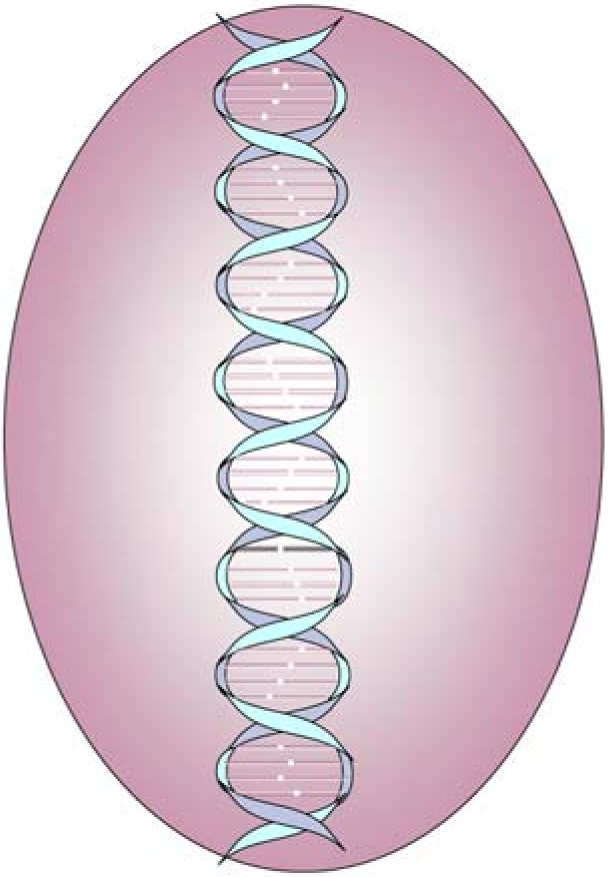
PRM-IT V3 Reference Library - A7 Resilience

PRM-IT Version 3.0
April, 2008

PRM - IT
IBM Process Reference Model for IT

Sequencing the DNA of IT Management



Copyright Notice

Trademarks

Notices

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to valid intellectual property or other legally protectable right of Tivoli Systems or IBM, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user. Tivoli Systems or IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

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

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

Details are provided for:

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

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

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

The PRM-IT Reference Library books

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

The nine reference manuals are A0 through A8. The *A0 Manage IT* book examines the context of the processes for IT, exploring the key external agents — stakeholders and their interactions with IT. The reference manuals A1 through A8 provide the complete description of all 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
- A0 Manage IT
- A1 Governance and Management System
- A2 Customer Relationships
- A3 Direction
- A4 Realization
- A5 Transition
- A6 Operations
- A7 Resilience
- A8 Administration
- IDEFØ Node Tree
- IDEFØ Diagrams
- PRM-IT Glossary

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.

[A7] Resilience

Description

Purpose

The Resilience category of processes describes the analysis and proactive planning required to enable resilient infrastructure, applications, and services. Resilience is here defined as the ability to absorb conditions or faults without service failure and the ability to quickly return to a previous good condition. Each process covers a range of activities from handling everyday adjustments as required by service operations through anticipating the potential future demands upon its specific domain.

In order to accomplish their collective mission, all processes require input from a wide range of other processes, including such items as architectural information, problem and known error information, solution designs, scheduled projects and changes, as well as operational monitoring data. Resilience processes use this input to establish ongoing resilience capabilities, ensuring service level attainment and customer satisfaction while controlling costs.

Rationale

All of the processes in this category analyze information from a variety of sources and then generate proactive plans to minimize risks associated with the potential failure of any component (or group of components) or human actor used to deliver services. The processes in this category are also responsible for ensuring compliance with (internal and external) laws and regulations, internal policies and procedures, as well as maintaining defined levels of security on information and IT services.

Value

- Ensures compliance with all security and regulatory considerations and requirements, reducing both IT and business risk
- Establishes proactive plans to ensure that infrastructure and application-based services are reliable, robust, secure, consistent and facilitate the efficient and effective support of business processes
- Provides the means to monitor both current IT system availability as well as to project future capacity requirements, improving IT's ability to support business direction
- Establishes responsibility for operation, management and maintenance of all physical facilities necessary to deliver services to the business
- Provides assurance that agreed to IT Services will continue to support business requirements in the event of a catastrophic disruption to the business environment

Controls

- Identity and Access Rights Register (From: A6 A67 A673 A674)
- IT Plan (From: A3 A36 A365)
- IT Strategy (From: A3 A31 A315)
- Service Catalog (From: A2 A23 A235)
- SLAs, OLAs, UCs (From: A2 A24 A243)
- IT Management Ecosystem (From: A1)
- Environment Information (From: outside the model)
- Business Strategy

- IT Budget (From: A8 A81 A813)

Inputs

- Architecture Baselines and Roadmaps (From: A3 A33 A334)
- Change Schedule (From: A5 A51 A515 A516)
- Service Metric Data and Reports (From: A6)
- Operational Monitoring Data (From: A6 A62 A622 A623 A624 A63 A633 A634 A635 A636)
- Incident Information (From: A6 A65 A657)
- Problem Information (From: A6 A66 A667)
- Stakeholder Requirements (From: A2 A21 A213)
- Solution_ Deployed (From: A5 A53 A536)
- Change Information (From: A5 A51 A518)
- Configuration Information (From: A5 A54 A544)
- Asset Information (From: A5 A55 A553)
- Solution Design (From: A4 A42 A425)
- Solution Plans and Commitments (From: A4 A41 A42 A422 A425 A43 A432 A44 A442 A45 A452)
- Business and IT Models (From: A3 A33 A333)
- Service Request_ Authorized (From: A6 A61 A613)
- Service Level Package (From: A2 A25 A255)
- Business Input (From: outside the model)

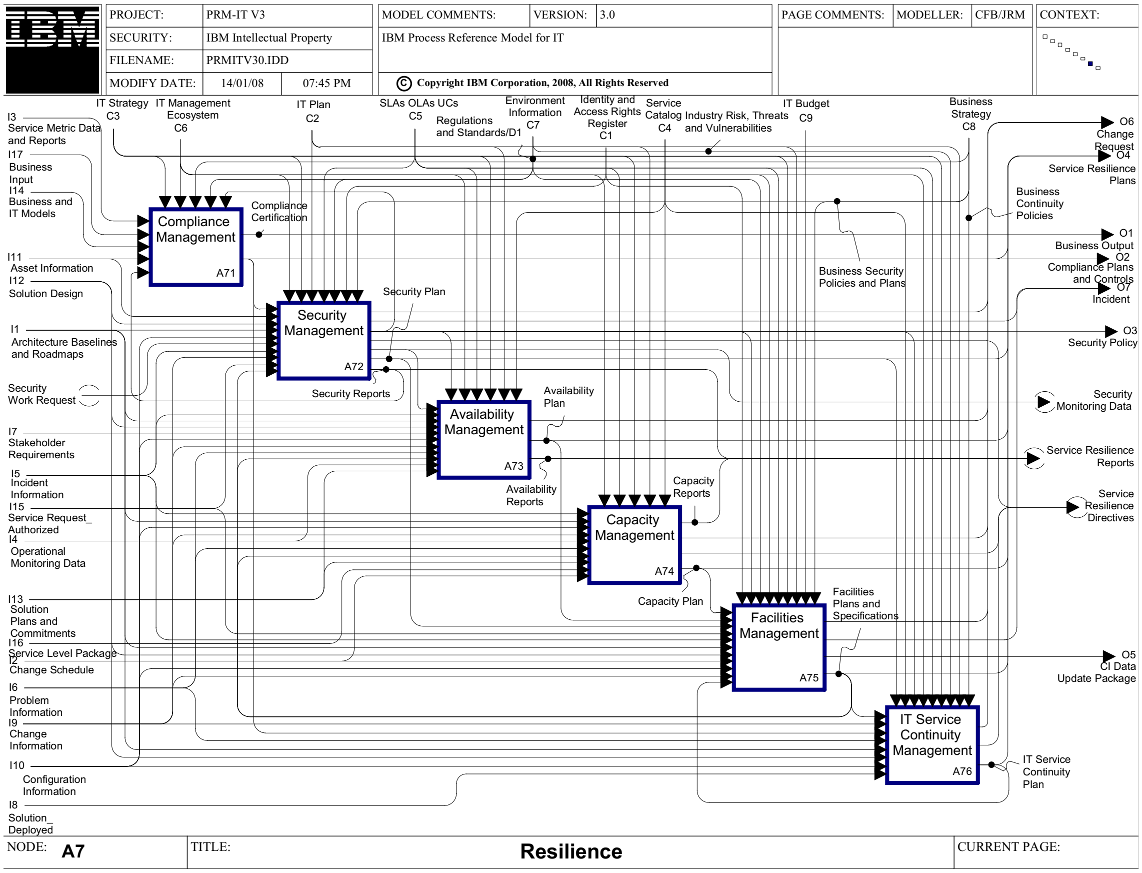
Outputs

- Business Output (To: Outside-the-Model)
- Compliance Plans and Controls (To: A1 A11 A111 A113 A114 A3 A36 A361 A37 A371 A4 A41 A412 A413 A5 A51 A511 A52 A521 A53 A531 A54 A545 A55 A554 A555 A6 A63 A632 A67 A671 A715 A716 A72 A725 A76 A763 A8 A81 A811)
- Security Policy (To: A2 A21 A213 A24 A243 A3 A31 A314 A33 A331 A332 A333 A34 A341 A342 A343 A4 A41 A413 A6 A67 A671 A672 A673 A674 A675 A71 A712 A713 A723 A724 A725 A726 A727 A73 A732 A75 A752 A76 A763 A8 A82 A822 A85 A852)
- Service Resilience Plans (To: A2 A22 A221 A24 A243 A246 A25 A255 A26 A265 A266 A3 A35 A353 A354 A36 A364 A5 A52 A522 A523 A53 A532 A6 A61 A611 A62 A621 A63 A632 A64 A641 A65 A651 A66 A661)
- CI Data Update Package (To: A5 A54 A542 A543)
- Change Request (To: A5 A51 A512)
- Incident (To: A537 A6 A65 A652)

Processes

This process category is composed of these processes:

- A71 Compliance Management
- A72 Security Management
- A73 Availability Management
- A74 Capacity Management
- A75 Facilities Management
- A76 IT Service Continuity Management



PROJECT:
PRM-IT V3
SECURITY:
IBM Intellectual Property
FILENAME:
PRMITV30.IDD
MODIFY DATE:
14/01/08
07:45 PM
MODEL COMMENTS:
VERSION:
3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER:
CFB/JRM
CONTEXT:
IT Strategy C3
IT Management Ecosystem C6
IT Plan C2
SLAs OLAs UCs C5
Regulations and Standards/D1
Environment Information C7
Identity and Access Rights Register C1
Service Catalog C4
Industry Risk, Threats and Vulnerabilities
IT Budget C9
Business Strategy C8
I3 Service Metric Data and Reports
I17 Business Input
I14 Business and IT Models
I11 Asset Information
I12 Solution Design
I1 Architecture Baselines and Roadmaps
Security Work Request
I7 Stakeholder Requirements
I5 Incident Information
I15 Service Request_ Authorized
I4 Operational Monitoring Data
I13 Solution Plans and Commitments
I16 Service Level Package
I2 Change Schedule
I6 Problem Information
I9 Change Information
I10 Configuration Information
I8 Solution_ Deployed
Compliance Management A71
Compliance Certification
Security Management A72
Security Plan
Security Reports
Availability Management A73
Availability Plan
Availability Reports
Capacity Management A74
Capacity Reports
Capacity Plan
Facilities Management A75
Facilities Plans and Specifications
IT Service Continuity Management A76
IT Service Continuity Plan
Business Security Policies and Plans
Business Continuity Policies
O6 Change Request
O4 Service Resilience Plans
O1 Business Output
O2 Compliance Plans and Controls
O7 Incident
O3 Security Policy
Security Monitoring Data
Service Resilience Reports
Service Resilience Directives
O5 CI Data Update Package
NODE: A7
TITLE:
Resilience
CURRENT PAGE:

Figure 1. A7 Resilience Diagram

[A71] Compliance Management

Purpose

The purpose of the Compliance Management process is to ensure adherence to laws and regulations, internal policies, procedures, and stakeholder commitments.

Outcomes

As a result of successful implementation of this process:

- Regulatory, audit, and other internal compliance is ensured and demonstrated
- Legal liabilities and related productivity losses consequential upon any compliance breach are avoided
- The reputation and value of the brand of the businesses that IT serves is protected

Scope

Integrity (sound operating) and compliance as an outcome across all of the IT endeavor's undertakings.

Includes

- Consideration of internal and external regulations, standards and legal obligations impacting the business where they could require IT support. For example:
  - Privacy regulations
  - Laws such as Sarbanes Oxley
  - Industry standards and guidelines such as ISO 27001 (ISO17799), COSO and CobiT
- Specification of compliance controls needed within IT services and solutions and also within other IT processes
- Internal and external audit readiness preparations
- Compliance audits

Excludes

- Setting internal policies (IT Governance and Management System Framework)
- Modification to IT services and solutions to establish compliance controls (through Realization and Deployment categories)
- Modification to other IT processes (through IT Governance and Management System categories)
- Operation of the defined compliance controls within the transactions of the IT endeavor. This responsibility becomes part of the activity of each relevant IT process

Controls

- IT Strategy (From: A3 A31 A315)

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

- IT Management Ecosystem (From: A1)

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

- Business Strategy

  The business strategy stated in terms of strategic intent, roadmap, drivers, objectives and policies.

- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- 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

- Service Metric Data and Reports (From: A6)

  Significant service delivery event logs, volume, and other measurement data relating to how effectively and efficiently services are provided by IT. 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.

- Business Input (From: outside the model)

  The various input items from the business to the IT provider that shape or direct the IT service. Examples of such inputs include:

  - Guidance
  - Instructions
  - General commentary and information about business operating conditions
- Business and IT Models (From: A3 A33 A333)

  Representations of relevant aspects of the business' activities, in model formats, and with or without the inclusion of related IT factors.

- Asset Information (From: A5 A55 A553)

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

- Security Reports (From: A72 A727)

  The reports from auditing and other analyses of IT security monitoring data.

Outputs

- Compliance Certification

  Formal declaration by the accountable executive of adherence to regulatory requirements.

- Compliance Plans and Controls (To: A1 A11 A111 A113 A114 A3 A36 A361 A37 A371 A4 A41 A412 A413 A5 A51 A511 A52 A521 A53 A531 A54 A545 A55 A554 A555 A6 A63 A632 A67 A671 A715 A716 A72 A725 A76 A763 A8 A81 A811)

  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.

Activities

This process is composed of these activities:

- A711 Establish Compliance Management Framework
- A712 Identify Compliance Requirements
- A713 Assess Compliance Requirements
- A714 Define Compliance Controls Plan
- A715 Implement Compliance Controls
- A716 Audit and Report Compliance
- A717 Evaluate Compliance Management Performance

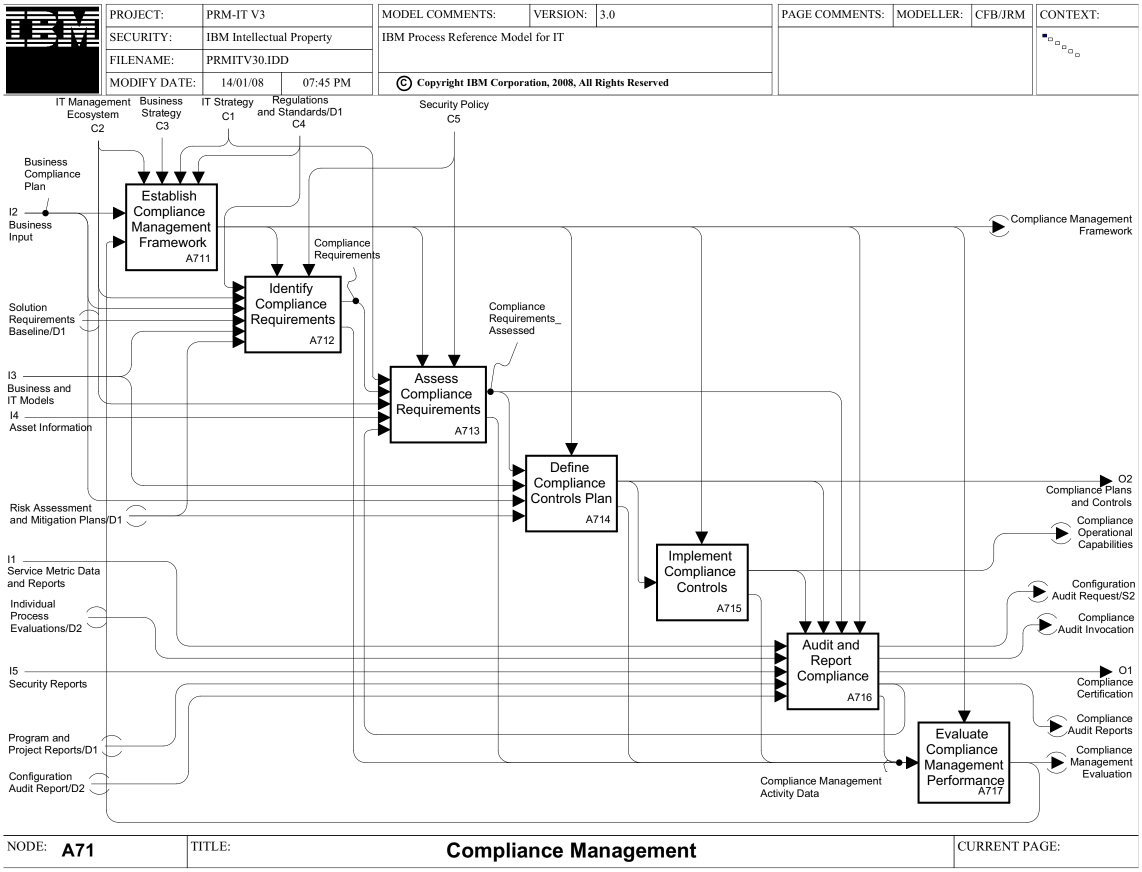

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS:
VERSION: 3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER: CFB/JRM
CONTEXT:
IT Management Ecosystem C2
Business Strategy C3
IT Strategy C1
Regulations and Standards/D1 C4
Security Policy C5
Business Compliance Plan
I2 Business Input
Establish Compliance Management Framework A711
Compliance Management Framework
Compliance Requirements
Identify Compliance Requirements A712
Solution Requirements Baseline/D1
Compliance Requirements_ Assessed
I3 Business and IT Models
I4 Asset Information
Assess Compliance Requirements A713
Define Compliance Controls Plan A714
O2 Compliance Plans and Controls
Risk Assessment and Mitigation Plans/D1
Compliance Operational Capabilities
I1 Service Metric Data and Reports
Implement Compliance Controls A715
Configuration Audit Request/S2
Individual Process Evaluations/D2
Compliance Audit Invocation
Audit and Report Compliance A716
I5 Security Reports
O1 Compliance Certification
Compliance Audit Reports
Program and Project Reports/D1
Evaluate Compliance Management Performance A717
Compliance Management Evaluation
Configuration Audit Report/D2
Compliance Management Activity Data
NODE: A71
TITLE: Compliance Management
CURRENT PAGE:

Figure 2. A71 Compliance Management

[A711] Establish Compliance Management Framework

Description

Based on the business and IT strategy and the policies and practices embodied within the IT management system, guidelines and a framework for Compliance Management have to be developed. The tasks in this activity include:

- Determining the requirements for the way compliance management process will be consistent with the overall business compliance approach
- Establishing the framework for Compliance Management by defining and implementing practices, procedures, and systems that support process activities
- Defining the strategy for Compliance Management tools and capabilities, and how they should be sourced. For instance, should they be developed in-house or rely more on vendor capabilities
- Defining evaluation criteria for Compliance Management solutions and services
- Determining skill requirements for the staff and assigning staff based on these systems

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

The establishment of the process framework also includes the continuous improvement of Compliance Management. For example, the consideration of the Compliance 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.
- Business Strategy

  The business strategy stated in terms of strategic intent, roadmap, drivers, objectives and policies.
- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)

Inputs

- Business Compliance Plan

  The compliance requirements determined by the business, derived by examination across the span of its activities and details of the specifications and implementations of corresponding compliance plans.

- Compliance Management Evaluation (From: A717)

  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

- Compliance Management Framework (To: A712 A713 A714 A715 A716 A717)

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

[A712] Identify Compliance Requirements

Description

This activity seeks out and collates the requirements for compliance. The requirements can be derived from several sources, including:

- The business, through the Business Compliance Plan
- External regulations and standards (with particular applicability to the design and operation of IT solutions)
- Internal IT policies

Controls

- Compliance Management Framework (From: A711)

  The policies, procedures, organizational roles and responsibilities and other information under which the Compliance 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

- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- 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 Compliance Plan

  The compliance requirements determined by the business, derived by examination across the span of its activities and details of the specifications and implementations of corresponding compliance plans.

- Solution Requirements Baseline (From: A41 A415)

  Established according to prescribed organizational standards, it is a baseline of all the Solution Requirements work products currently under Configuration Management.

- Business and IT Models (From: A3 A33 A333)

  Representations of relevant aspects of the business' activities, in model formats, and with or without the inclusion of related IT factors.

- Risk Assessment and Mitigation Plans (From: A34)

  The recommendations as to the acceptability or otherwise of the risk factors of any undertaking (such as projects, external development) and the risk limitation measures selected to reduce the impact of unacceptable risk occurrence.

Outputs

- Compliance Requirements (To: A713)

  The necessary conditions and actions needed to adhere to external regulations or standard practices and also to requirements established by the business through activities such as audit and oversight.

- Compliance Management Activity Data (To: A717)

  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.

[A713] Assess Compliance Requirements

Description

Assessment of identified compliance requirements to establish exactly which of the potential compliance aspects must be put into effect, and to what degree. In a fashion similar to Risk Assessment, it includes evaluating the costs of compliance against the consequences of noncompliance. The output will be the base from which all compliance controls are built.

Controls

- Compliance Management Framework (From: A711)

  The policies, procedures, organizational roles and responsibilities and other information under which the Compliance 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

- IT Strategy (From: A3 A31 A315)

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

- Compliance Requirements (From: A712)

  The necessary conditions and actions needed to adhere to external regulations or standard practices and also to requirements established by the business through activities such as audit and oversight.
- 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.
- Asset Information (From: A5 A55 A553)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.
- Compliance Audit Reports (From: A716)

  Documents communicating the results of individual process compliance and mitigation audits.

Outputs

- Compliance Requirements_ Assessed (To: A714 A716)

  Sets of categorized, quantified, and prioritized compliance items that the IT endeavor must address. Also includes any compliance requirements for which noncompliance has been assessed, with decision reasons and analysis of likely consequences.
- Compliance Management Activity Data (To: A717)

  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.

[A714] Define Compliance Controls Plan

Description

The compliance controls that must be put into effect are specified and designed. Compliance controls identified here must be consistent with the overall business compliance plan and also provide the basis by which the IT executives will be able to attest (certify) that the IT endeavor has met compliance requirements specific to IT undertakings.

Controls

- Compliance Management Framework (From: A711)

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

Inputs

- Compliance Requirements_ Assessed (From: A713)

  Sets of categorized, quantified, and prioritized compliance items that the IT endeavor must address. Also includes any compliance requirements for which noncompliance has been assessed, with decision reasons and analysis of likely consequences.
- Business and IT Models (From: A3 A33 A333)

  Representations of relevant aspects of the business' activities, in model formats, and with or without the inclusion of related IT factors.

- Business Compliance Plan

  The compliance requirements determined by the business, derived by examination across the span of its activities and details of the specifications and implementations of corresponding compliance plans.
- Risk Assessment and Mitigation Plans (From: A34)

  The recommendations as to the acceptability or otherwise of the risk factors of any undertaking (such as project, external development) and the risk limitation measures selected to reduce the impact of unacceptable risk occurrence.

Outputs

- Compliance Plans and Controls (To: A1 A11 A111 A113 A114 A3 A36 A361 A37 A371 A4 A41 A412 A413 A5 A51 A511 A52 A521 A53 A531 A54 A545 A55 A554 A555 A6 A63 A632 A67 A671 A715 A716 A72 A725 A76 A763 A8 A81 A811)

  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.
- Compliance Management Activity Data (To: A717)

  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.

[A715] Implement Compliance Controls

Description

The overseeing of the development and deployment of defined compliance controls. The outcome is that the compliance controls are in operation across all relevant IT activities.

Controls

- Compliance Management Framework (From: A711)

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

Inputs

- 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.

Outputs

- Compliance Operational Capabilities (To: A716)

  The set of capabilities which implement the various controls required to adhere to specific regulatory or more informally generated requirements.
- Compliance Management Activity Data (To: A717)

  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.

[A716] Audit and Report Compliance

Description

Compliance control activities and outcomes are monitored and analyzed for progress and certification. Exposures and findings that are discovered during the audit will be documented and communicated to ensure compliance. Where required, conformance will be formally certified: for example, SOX Attestation. Reports are produced on any aspect of compliance workings.

Controls

- Compliance Operational Capabilities (From: A715)

  The set of capabilities which implement the various controls required to adhere to specific regulatory or more informally generated requirements.
- 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.
- Compliance Requirements_ Assessed (From: A713)

  Sets of categorized, quantified, and prioritized compliance items that the IT endeavor must address. Also includes any compliance requirements for which noncompliance has been assessed, with decision reasons and analysis of likely consequences.
- Compliance Management Framework (From: A711)

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

Inputs

- Service Metric Data and Reports (From: A6)

  Significant service delivery event logs, volume, and other measurement data relating to how effectively and efficiently services are provided by IT. 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.
- Individual Process Evaluations

  A collection of metrics which describe the effectiveness and efficiency of an individual process.

- Security Reports (From: A72 A727)

  The reports from auditing and other analyses of IT security monitoring data.
- Program and Project Reports (From: A37)

  The body of information ranging from formal, regular and summarized, through informal, ad hoc, and detailed about any aspect of program and project status, and plans. It is available to any process with a need to know.
- Configuration Audit Report (From: A545)

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

Outputs

- Configuration Audit Request (To: A545)

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

  A directive to all processes that are required to operate under the risk and compliance controls for evidence which will be examined to identify whether and how well those controls are being operated.
- Compliance Certification

  Formal declaration by the accountable executive of adherence to regulatory requirements.
- Compliance Audit Reports (To: A143 A713)

  Documents communicating the results of individual process compliance and mitigation audits.
- Compliance Management Activity Data (To: A717)

  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.

[A717] Evaluate Compliance Management Performance

Description

The evaluation of the performance of the process aims at identifying areas of the overall process requiring improvement. This covers the foundation and interfaces of the process, all activities, their accomplishments, their degree of automation, as well as the roles and responsibilities including the respective skills. The bases for improvements are insights and the lessons learned from the observations and analysis of activity accomplishments and results.

Controls

- Compliance Management Framework (From: A711)

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

Inputs

- Compliance Management Activity Data (From: A712 A713 A714 A715 A716)

  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

- Compliance Management Evaluation (To: A711)

  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.

[A72] Security Management

Purpose

The purpose of the Security Management process is to establish and operate security controls and protections over all IT assets and services in order to conform to overall business security as well as IT-specific requirements. It includes activities to mitigate the risk posed by malicious outsiders and insiders, and to decrease vulnerabilities in the IT services, systems and processes that would make it easier for such malicious parties to succeed.

Outcomes

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

- The confidentiality, integrity, and accessibility of information meets agreed requirements:
  - Information is available for approved purposes
  - Access (whether internal or external) to protected items can be validated and tracked
  - Information and systems are protected from unauthorized access and any attacks
- IT services and infrastructure meet external security requirements from service level agreements, contracts, and legislative dictates
- IT security aligns with the business' overall security requirements
- The reputation of the business as secure and trustworthy is protected

Scope

The process covers the life cycle of security concerns, including planning, operational measures, evaluation, and audit. It will identify IT security threats, vulnerabilities, and risks in order to develop an overall approach to counter and handle them that is aligned with business security requirements. It will operate security protections and mechanisms which meet the desired level of confidentiality, availability and integrity for information and IT services.

Includes

- Information security policy
- Specification of information security controls including asset use, access, documentation, and information controls and overseeing their establishment
- Operation of controls and measures such as:
  - Credential operations
  - Perimeter defense
  - Intrusion detection
  - Secure coding standards
  - Key and encryption management
  - Separation of duties
  - Application isolation
- Identification of IT security incidents
- Management of supplier and partner access to services and systems
- Compliance enforcement measures (related to security)

Excludes

- Establishment and maintenance of identities and access rights (Identity and Access Management)
- Health and safety (Business responsibility, with contribution from Facilities Management)
- Business security management, including trust management as it relates to business processes (Business responsibility)
- Identification of privacy requirements (within the scope of Compliance 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.
- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.
- IT Plan (From: A3 A36 A365)

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

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

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[1]
  - 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.”[2]
  - 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

[1] ITIL V3 Glossary

[2] ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[3]

These agreements can be in a draft or finalized status.

- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- Identity and Access Rights Register (From: A6 A67 A673 A674)

  The records that 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).
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.

Inputs

- 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.
- Asset Information (From: A5 A55 A553)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.
- 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.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Configuration 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 Work Request (From: A535 A623 A624)

  A Security Request originating from another process.

[3] 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.
- 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 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.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

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. (To: A537 A6 A65 A652)Incident

  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.
- Security Policy (To: A2 A21 A213 A24 A243 A3 A31 A314 A33 A331 A332 A333 A34 A341 A342 A343 A4 A41 A413 A6 A67 A671 A672 A673 A674 A675 A71 A712 A713 A723 A724 A725 A726 A727 A73 A732 A75 A752 A76 A763 A8 A82 A822 A85 A852)

  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.
- Service Resilience Directives (To: A62 A622 A623 A63 A632)

  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.
- Security Monitoring Data (To: A64 A642 A67 A675 A727 A73 A735)

  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.
- Security Plan (To: A33 A334 A335 A336 A34 A344 A345 A346 A42 A422 A423 A424 A44 A442 A612 A613 A67 A671 A75 A752 A76 A764 A843)

  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).
- Security Reports (To: A346 A71 A716 A723 A725)

  The reports from auditing and other analyses of IT security monitoring data.

Activities

This process is composed of these activities:

- A721 Establish Security Management Framework
- A722 Produce and Maintain Security Policy
- A723 Analyze Security Threats, Vulnerabilities and Risks
- A724 Classify Information Asset Security
- A725 Plan and Implement Security Practices
- A726 Operate Security Protection Mechanisms
- A727 Monitor, Assess, Audit and Report Security
- A728 Evaluate Security Management Performance

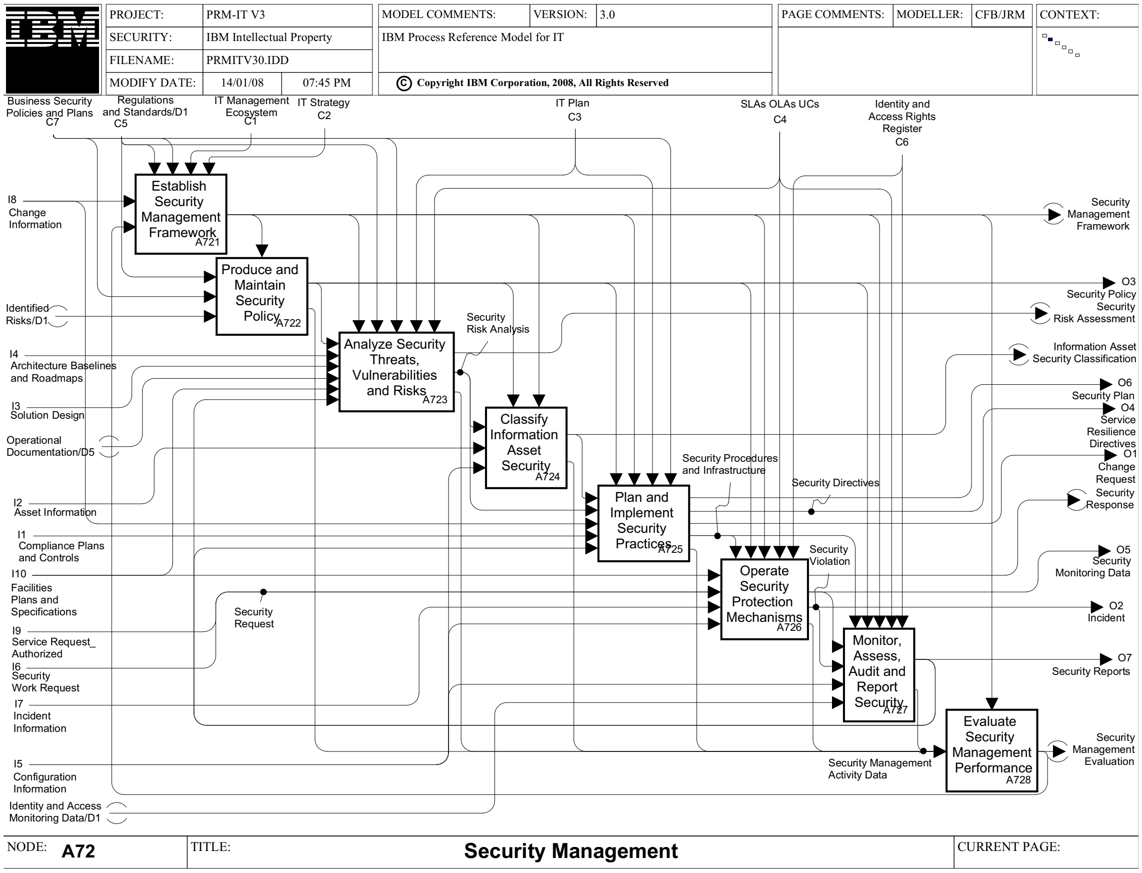

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS:
VERSION: 3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER: CFB/JRM
CONTEXT:
Business Security Policies and Plans C7
Regulations and Standards/D1 C5
IT Management Ecosystem C1
IT Strategy C2
IT Plan C3
SLAs OLAs UCs C4
Identity and Access Rights Register C6
I8 Change Information
Identified Risks/D1
I4 Architecture Baselines and Roadmaps
I3 Solution Design
Operational Documentation/D5
I2 Asset Information
I1 Compliance Plans and Controls
I10 Facilities Plans and Specifications
I9 Service Request_ Authorized
I6 Security Work Request
I7 Incident Information
I5 Configuration Information
Identity and Access Monitoring Data/D1
Establish Security Management Framework A721
Produce and Maintain Security Policy A722
Analyze Security Threats, Vulnerabilities and Risks A723
Classify Information Asset Security A724
Plan and Implement Security Practices A725
Operate Security Protection Mechanisms A726
Monitor, Assess, Audit and Report Security A727
Evaluate Security Management Performance A728
Security Risk Analysis
Security Request
Security Procedures and Infrastructure
Security Directives
Security Violation
Security Management Activity Data
Security Management Framework
O3 Security Policy
Security Risk Assessment
Information Asset Security Classification
O6 Security Plan
O4 Service Resilience Directives
O1 Change Request
Security Response
O5 Security Monitoring Data
O2 Incident
O7 Security Reports
Security Management Evaluation
NODE: A72
TITLE: Security Management
CURRENT PAGE:

Figure 3. A72 Security Management

[A721] Establish Security Management Framework

Description

The purpose is define and maintain a framework of policies and procedures that guides and governs the behavior of the Security Management process and its activities. Incorporate mandatory elements from the Management Ecosystem, and define a set of metrics to be used by each process for measurement and reporting of performance. It also must review the process evaluation based on analysis of current performance, and approve recommendations for improvements. Finally, to refine the metrics to encourage process vitality and cost effectiveness, an to incorporate updated metrics and process change recommendations into the framework and communicate the changes.

Controls

- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.
- 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 Strategy (From: A3 A31 A315)

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

Inputs

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.
- Security Management Evaluation (From: A728)

  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

- Security Management Framework (To: A331 A341 A722 A723 A724 A725 A726 A727 A728 A751 A761)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

[A722] Produce and Maintain Security Policy

Description

This activity creates the overall statement of the aims and objectives for the security that is to be established and operated in relation to IT services and resources, and maintains its currency as circumstances change for both the IT service provider and its customer set. It works within the limits set for the security policy of the parent business, modifying or extending its coverage to include aspects specific to information technology.

Controls

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

Inputs

- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.
- Identified Risks (From: A342)

  Areas in the business where there is a potential for realization of unwanted, adverse consequences if an event or a given set of events occurs.

Outputs

- Security Policy (To: A2 A21 A213 A24 A243 A3 A31 A314 A33 A331 A332 A333 A34 A341 A342 A343 A4 A41 A413 A6 A67 A671 A672 A673 A674 A675 A71 A712 A713 A723 A724 A725 A726 A727 A73 A732 A75 A752 A76 A763 A8 A82 A822 A85 A852)

  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.
- Security Management Activity Data (To: A728)

  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.

[A723] Analyze Security Threats, Vulnerabilities and Risks

Description

Identify security threats, determine risks and vulnerabilities which effect the IT organization or that IT can affect, and recommend mitigating changes based on this analysis.

Controls

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.
- IT Plan (From: A3 A36 A365)

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

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

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[4]
  - 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.” [5]
  - 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

[4] ITIL V3 Glossary

[5] ITIL V3 Glossary

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

These agreements can be in a draft or finalized status.

Inputs

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

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Solution Design (From: A4 A42 A425)

  Solution design, including conceptual, macro, and micro designs, together with identified issues and risks, and formally validated and approved (signed off) by the key stakeholders. It not only covers all the functional and non-functional requirements of the solution, but also the design for meeting the compliance reporting requirements applicable to the solution.
- 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.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- Security Reports (From: A72 A727)

  The reports from auditing and other analyses of IT security monitoring data.

Outputs

- Security Risk Assessment (To: A42 A424 A425 A44 A444 A445 A45 A454 A455)

  A detailed analysis of the current and projected security risk factors facing the enterprise.
- Security Risk Analysis (To: A724 A725)

  The results and recommendations of an in-depth study of the threats, vulnerabilities and risk factors to be mitigated by security practices and protection mechanisms.
- Security Management Activity Data (To: A728)

  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.

[A724] Classify Information Asset Security

Description

Develop a security classification scheme for information assets by examining the inventory. The scheme identifies the required level of security for each categorization.

Controls

- 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.
- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

Inputs

- Security Risk Analysis (From: A723)

  The results and recommendations of an in-depth study of the threats, vulnerabilities and risk factors to be mitigated by security practices and protection mechanisms.
- Asset Information (From: A5 A55 A553)

  Could be reports, covering multiple asset items, or just the specific information on an individual asset.
- Configuration Information (From: A5 A54 A544)

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

Outputs

- Information Asset Security Classification (To: A725)

  The level of protection to be established and operated against each category of information assets. It includes:

  - Identification of ownership requirements
  - Handling and labeling procedures
- Security Management Activity Data (To: A728)

  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.

[A725] Plan and Implement Security Practices

Description

This activity establishes the Security plan. It defines and creates an appropriate security infrastructure and procedures, translates actions in the plan to security directives, and communicates them. It also makes request changes in the environment to realize the Security plan.

Controls

- 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.
- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.
- 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.
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.

Inputs

- Information Asset Security Classification (From: A724)

  The level of protection to be established and operated against each category of information assets. It includes:

  - Identification of ownership requirements
  - Handling and labeling procedures
- Security Risk Analysis (From: A723)

  The results and recommendations of an in-depth study of the threats, vulnerabilities and risk factors to be mitigated by security practices and protection mechanisms.
- 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.

- 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.
- Security Reports (From: A72 A727)

  The reports from auditing and other analyses of IT security monitoring data.

Outputs

- Security Plan (To: A33 A334 A335 A336 A34 A344 A345 A346 A42 A422 A423 A424 A44 A442 A612 A613 A67 A671 A75 A752 A76 A764 A843)

  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).
- Security Directives (To: A333 A334 A67 A673 A674)

  The directive to take action, or the action to be taken, so that the protections which implement the desired security practices are properly operated.
- 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.
- Security Procedures and Infrastructure (To: A726 A727)

  The collected design, components, policies and direction which together establish an infrastructure to be put into place for security management.
- Security Management Activity Data (To: A728)

  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.

[A726] Operate Security Protection Mechanisms

Description

This activity puts in place prescribed security controls and procedures throughout all aspects of IT, both in terms of the IT organization and by activating the security protections within IT solutions and services.

Applying the mechanisms involves the full range of education and training, installing new systems, and testing to make sure that security controls and procedures work properly.

This activity actuates and monitors the full range of security measures and capabilities, responding to service or resource access authorization requests in addition to noting security violations and initiating incidents when necessary.

Real-time intrusion detection sensing and immediate responses are an important part of the function of this activity.

Controls

- Security Procedures and Infrastructure (From: A725)

  The collected design, components, policies and direction which together establish an infrastructure to be put into place for security management.

- 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.

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

- 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.”[6]
  - 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.”[7]
  - 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.”[8]

  These agreements can be in a draft or finalized status.

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

  The records that 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).

[6] ITIL V3 Glossary

[7] ITIL V3 Glossary

[8] ITIL V3 Glossary

Inputs

- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- Security Request (From: A634)

  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
- 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.
- Configuration Information (From: A5 A54 A544)

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

Outputs

- Security Response (To: A535 A623 A624 A634)

  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
- Security Monitoring Data (To: A64 A642 A67 A675 A727 A73 A735)

  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.
- Security Violation (To: A727)

  An event (an activity or state) that is inconsistent with defined security practices and requires further inspection and evaluation.
- Security Management Activity Data (To: A728)

  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.

[A727] Monitor, Assess, Audit and Report Security

Description

This activity addresses reviewing security controls and mechanisms and determining whether they appropriately and effectively implement security policies and procedures as described in the Security Management Framework and the Security plan.

Controls

- Security Procedures and Infrastructure (From: A725)

  The collected design, components, policies and direction which together establish an infrastructure to be put into place for security management.

- 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.

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

- 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.

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

  The records that 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).

[9] ITIL V3 Glossary
[10] ITIL V3 Glossary
[11] ITIL V3 Glossary

Inputs

- 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.

- Security Violation (From: A726)

  An event (an activity or state) that is inconsistent with defined security practices and requires further inspection and evaluation.

- 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.

Outputs

- Security Reports (To: A346 A71 A716 A723 A725)

  The reports from auditing and other analyses of IT security monitoring data.

- Security Management Activity Data (To: A728)

  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.

[A728] Evaluate Security Management Performance

Description

The evaluation of Security Management 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

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.

Inputs

- Security Management Activity Data (From: A722 A723 A724 A725 A726 A727)

  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

- Security Management Evaluation (To: A721)

  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.

[A73] Availability Management

Purpose

The purpose of Availability Management is to match the availability of the IT services against the current and future identified needs of the business or to exceed them.   Availability Management enhances the availability of services by planning long-term service availability, measuring and monitoring service availability, and formulating service availability design criteria that meet requirements.

Definition of availability: “Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.”[12]

Outcomes

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

- IT infrastructure provides a consistent level of availability that enables the business to meet its current and future objectives
- Availability related incidents and problems are minimized
- The provided level of availability is cost justified and optimized

Scope

ITIL defines components of availability to be:

- Reliability – “A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption.”[13]
- Maintainability – "A measure of how quickly and Effectively a Configuration Item or IT Service can be restored to normal working after a Failure. Maintainability is also used in the context of Software or IT Service Development to mean ability to be Changed or Repaired easily."[14]
- Serviceability – "The ability of a Third Party Supplier to meet the terms of their Contract. This Contract will include agreed levels of Reliability, Maintainability or Availability for a Configuration Item."[15]

Includes

- Availability needs and requirements
- Identification of capabilities needed to meet requirements
- New and existing IT services
- Ensuring that availability provision of underlying services and suppliers in support of primary IT services is factored in
- Considering all aspects of IT service delivery and support that could impact availability (training, tools)

[12] ITIL V3 Glossary
[13] ITIL V3 Glossary
[14] ITIL V3 Glossary
[15] ITIL V3 Glossary

Excludes

- Business Continuity Management or disaster recovery (Business responsibility along with IT Service Continuity Management)
- Direct handling of service failures (Incident Management)
- Approval of capabilities needed to meet requirements (Portfolio Management)
- Creation of capabilities needed to meet requirements (Realization category of processes)
- Managing suppliers (Supplier Management)

Controls

- 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.
- 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.”[16]
  - 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.”[17]
  - 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.”[18]

  These agreements can be in a draft or finalized status.

[16] ITIL V3 Glossary
[17] ITIL V3 Glossary
[18] ITIL V3 Glossary

- IT Strategy (From: A3 A31 A315)

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

- IT 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."[19]

Inputs

- 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.

- 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.

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

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

- Solution Design (From: A4 A42 A425)

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

- Stakeholder Requirements (From: A2 A21 A213)

  The qualified needs for IT services that are to be progressed through the Portfolio process for decision making.

  These needs might be in a form suitable for direct translation into solution requirements and should include stakeholders' acceptance criteria.

- Configuration Information (From: A5 A54 A544)

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

- Change Information (From: A5 A51 A518)

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

[19] 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.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- 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.
- 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.

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.
- Availability Plan (To: A75 A752)

  A forward-looking plan aimed at improving the overall availability of the IT infrastructure within cost constraints.
- Availability Reports (To: A736 A737)

  Statistics expressed on how well the IT Infrastructure has met the needs of the business in availability terms. Might be included in Service achievement reports.

Activities

This process is composed of these activities:

- A731 Establish Availability Management Framework
- A732 Determine Availability Requirements
- A733 Formulate Availability and Recovery Design Criteria
- A734 Define and Implement Availability Targets and Related Measures
- A735 Monitor, Analyze and Report Availability
- A736 Investigate Unavailability
- A737 Produce Availability Plan
- A738 Evaluate Availability Management Performance

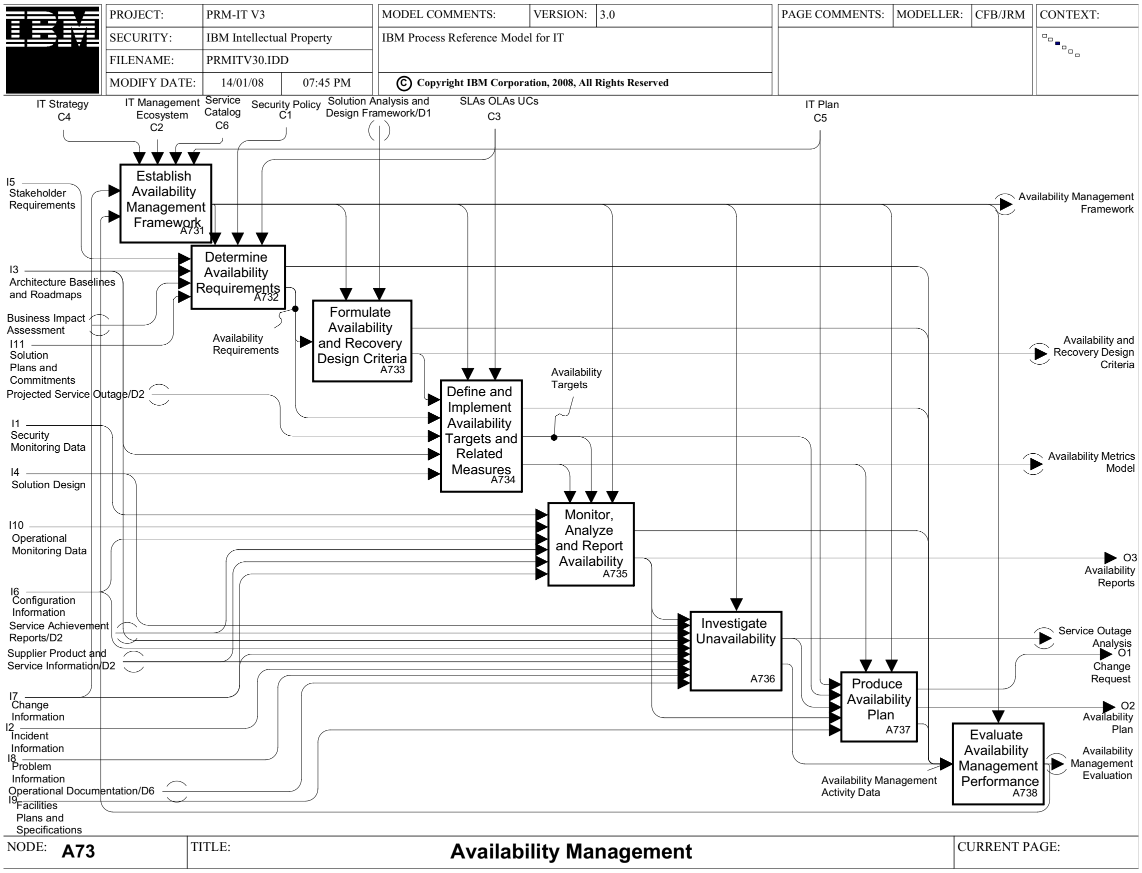

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS: VERSION: 3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER: CFB/JRM
CONTEXT:
IT Strategy C4
IT Management Ecosystem C2
Service Catalog C6
Security Policy C1
Solution Analysis and Design Framework/D1
SLAs OLAs UCs C3
IT Plan C5
I5 Stakeholder Requirements
I3 Architecture Baselines and Roadmaps
Business Impact Assessment
I11 Solution Plans and Commitments
Projected Service Outage/D2
I1 Security Monitoring Data
I4 Solution Design
I10 Operational Monitoring Data
I6 Configuration Information
Service Achievement Reports/D2
Supplier Product and Service Information/D2
I7 Change Information
I2 Incident Information
I8 Problem Information
Operational Documentation/D6
I9 Facilities Plans and Specifications
Establish Availability Management Framework A731
Determine Availability Requirements A732
Availability Requirements
Formulate Availability and Recovery Design Criteria A733
Define and Implement Availability Targets and Related Measures A734
Availability Targets
Monitor, Analyze and Report Availability A735
Investigate Unavailability A736
Produce Availability Plan A737
Evaluate Availability Management Performance A738
Availability Management Activity Data
Availability Management Framework
Availability and Recovery Design Criteria
Availability Metrics Model
O3 Availability Reports
Service Outage Analysis
O1 Change Request
O2 Availability Plan
Availability Management Evaluation
NODE: A73
TITLE: Availability Management
CURRENT PAGE:

Figure 4. A73 Availability Management

[A731] Establish Availability Management Framework

Description

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

- Understanding the requirements and specifications for availability management
- Defining the strategy for availability management tools and capabilities, and how they should be sourced. For instance, should they be developed in-house or rely more on vendor capabilities
- Specifying the data model for an Availability Management Information System:
  - Defined by ITIL as: “A virtual repository of all Availability Management data, usually stored in multiple physical locations.”[20]
- Defining evaluation criteria for availability management solutions and services
- Establishing the framework for Availability Management by defining and implementing practices and systems that support process activities
- Determining skill requirements for the staff, and assigning staff based on these systems

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

[20] ITIL V3 Glossary

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

Controls

- IT Strategy (From: A3 A31 A315)

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

- IT Management Ecosystem (From: A1)

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

- 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.”[21]

- 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

- 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.

- Availability Management Evaluation (From: A738)

  An analysis of how well the Availability Management process was performed. This can also include proposed modifications to the Availability Management Framework.

Outputs

- Availability Management Framework (To: A732 A733 A734 A735 A736 A737 A738)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

[21] ITIL V3 Glossary

[A732] Determine Availability Requirements

Description

This activity addresses the translation of business user and IT stakeholder requirements into quantifiable availability terms and conditions and targets, and then into availability-specific requirements that eventually contribute to the Availability Plan.

Controls

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

- 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.

- 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.”[22]
  - 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.”[23]

  These agreements can be in a draft or finalized status.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.”[24]

[22] ITIL V3 Glossary

[23] ITIL V3 Glossary

[24] ITIL V3 Glossary

Inputs

- Stakeholder Requirements (From: A2 A21 A213)

  The qualified needs for IT services that are to be progressed through the Portfolio process for decision making.

  These needs might be in a form suitable for direct translation into solution requirements and should include stakeholders' acceptance criteria.
- 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.
- Business Impact Assessment

  An appraisal of the impact of service unavailability on the business.
- 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.

Outputs

- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.
- Availability Requirements (To: A733 A734)

  An examination of the requirements for availability as expressed by the various stakeholders. As there might be some contention between these, this process must establish the definitive set of availability requirements which will influence solution and service development and operation.

[A733] Formulate Availability and Recovery Design Criteria

Description

This activity endeavors to understand the vulnerabilities to failure of a given IT infrastructure design, and to present design criteria that optimize the availability characteristics of solutions in the IT environment, including recovery capabilities.

Controls

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.
- Solution Analysis and Design Framework (From: A421)

  The logical structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for solution analysis and design.

Inputs

- Availability Requirements (From: A732)

  An examination of the requirements for availability as expressed by the various stakeholders. As there might be some contention between these, this process must establish the definitive set of availability requirements which will influence solution and service development and operation.

Outputs

- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.
- Availability and Recovery Design Criteria (To: A243 A422 A734 A764)

  General solution design principles that enhance service availability and recovery. This information is used to create or update solutions so that they are more resilient.

[A734] Define and Implement Availability Targets and Related Measures

Description

This activity is responsible for the negotiation of achievable availability targets with the business, based on business needs and priorities balanced with current IT capabilities and capacity. Both business application and IT infrastructure elements should be taken into consideration as targets are set.

In parallel, the activity represents availability measurement needs (through the Availability Plan) so that appropriate measurement and reporting capabilities can be established and ready to support monitoring and reporting of availability achieved against the targets.

Finalizing targets and associated mechanisms in place usually requires a cycle of feasibility interactions rather than being completed in a single pass.

Controls

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.
- 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.”[25]

- 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."[26]
- 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."[27]

These agreements can be in a draft or finalized status.

Inputs

- Availability and Recovery Design Criteria (From: A733)

  General solution design principles that enhance service availability and recovery. This information is used to create or update solutions so that they are more resilient.
- Availability Requirements (From: A732)

  An examination of the requirements for availability as expressed by the various stakeholders. As there might be some contention between these, this process must establish the definitive set of availability requirements which will influence solution and service development and operation.
- Projected Service Outage (From: A515)

  As defined in ITIL: "A Document that identifies the effect of planned Changes, maintenance Activities and Test Plans on agreed Service Levels."[28]
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Solution Design (From: A4 A42 A425)

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

Outputs

- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.
- Availability Targets (To: A735 A737)

  Objectives for service availability, typically focusing on service unavailability and business impact.
- Availability Metrics Model (To: A735 A737)

  The range of availability metrics and areas of reporting that are used to describe service availability.

[25] ITIL V3 Glossary
[26] ITIL V3 Glossary
[27] ITIL V3 Glossary
[28] ITIL V3 Glossary

[A735] Monitor, Analyze and Report Availability

Description

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify availability trends and issues.

Configuration information is used to generate detailed service component availability reporting as well as a perspective on overall service availability.

Controls

- Availability Metrics Model (From: A734)

  The range of availability metrics and areas of reporting that are used to describe service availability.
- Availability Targets (From: A734)

  Objectives for service availability, typically focusing on service unavailability and business impact.
- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

Inputs

- 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.
- 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.
- 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 Achievement Reports (From: A24 A244)

  One or more reports about how well the service levels have been achieved and which compare IT's actual service level results achieved against the service level standards and any specific service level targets negotiated with customers. The reports can include details of service impacts – both directly measured and an assessment of business impact. Some sections will be for customer distribution and others can be for service provider receipt only.
- 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 supply 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.
- 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.

Outputs

- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.

- Availability Reports (To: A736 A737)

  Statistics expressed on how well the IT Infrastructure has met the needs of the business in availability terms. Might be included in Service achievement reports.

[A736] Investigate Unavailability

Description

The detailed investigation by this activity is performed to identify the underlying causes (not just the symptoms) of any single incident, or set of related incidents, which have resulted in significant service unavailability.

The Service Outage Analysis' resultant recommendations might raise one of more RFCs to address these underlying causes.

Controls

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

Inputs

- Availability Reports (From: A73 A735)

  Statistics expressed on how well the IT Infrastructure has met the needs of the business in availability terms. Might be included in Service achievement reports.

- 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 Achievement Reports (From: A24 A244)

  One or more reports about how well the service levels have been achieved and which compare IT's actual service level results achieved against the service level standards and any specific service level targets negotiated with customers. The reports can include details of service impacts – both directly measured and an assessment of business impact. Some sections will be for customer distribution and others can be for service provider receipt only.

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

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

- Configuration Information (From: A5 A54 A544)

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

- Change Information (From: A5 A51 A518)

  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.

- 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 supply 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.
- 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.
- 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

- Service Outage Analysis (To: A664 A737)

  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.
- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.

[A737] Produce Availability Plan

Description

This activity generates the consolidated Availability Plan that summarizes resource availability optimization decisions and commitments for the planning period. It includes availability profiles, availability targets, availability issues descriptions, historical analyses of achievements with regard to targets summaries, and documents useful lessons learned. The Availability Plan is a comprehensive record of IT's approach and success in meeting user expectations for IT resource availability.

Controls

- Availability Metrics Model (From: A734)

  The range of availability metrics and areas of reporting that are used to describe service availability.

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

Inputs

- 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.
- Availability Targets (From: A734)

  Objectives for service availability, typically focusing on service unavailability and business impact.
- 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.
- Availability Reports (From: A73 A735)

  Statistics expressed on how well the IT Infrastructure has met the needs of the business in availability terms. Might be included in Service achievement reports.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

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.
- Availability Plan (To: A75 A752)

  A forward-looking plan aimed at improving the overall availability of the IT infrastructure within cost constraints.
- Availability Management Activity Data (To: A738)

  Results and metrics that describe the results of performing the Availability Management process.

[A738] Evaluate Availability Management Performance

Description

The evaluation of Evaluate Availability Management process performance identifies areas that need improvement. For example, 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

- Availability Management Framework (From: A731)

  The set of policies, procedures and mechanisms for performing the Availability Management process.

Inputs

- Availability Management Activity Data (From: A732 A733 A734 A735 A736 A737)

  Results and metrics that describe the results of performing the Availability Management process.

Outputs

- Availability Management Evaluation (To: A731)

  An analysis of how well the Availability Management process was performed. This can also include proposed modifications to the Availability Management Framework.

[A74] Capacity Management

Purpose

The purpose of Capacity Management is to match the capacity of the IT services and infrastructure to the current and future identified needs of the business. Capacity Management focuses on the complete spectrum from design and planning of service capacities through the operational aspects of service capacity.

Definition of Capacity: “The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.”[29]

Outcomes

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

- IT always has the capacity to meet the expected (agreed) current and future identified needs of the business
- Scalability requirements of the business are understood and accommodated
- Incidents caused by lack of capacity are averted
- The cost of capacity acquisition is reduced by planning and optimizing capacity usage.

Scope

The process covers a wide range: understanding service requirements, determining component capacities, the design and deployment of capacity, and meeting expectations. It collects and analyzes data that is relevant to application and infrastructure utilization and performance for the purpose of determining whether there are potential problems and issues that need to be addressed.

ITIL defines three focus areas which are addressed by Capacity Management. Each uses the primary activities of the process decomposition in differing ways, to differing end results.

- Business Capacity Management
  - This focus area is responsible for ensuring that the impacts of future business requirements for IT services upon IT resources are considered, planned, and implemented in a timely fashion
- Service Capacity Management
  - This focus area is the management of the performance of the IT services used by the customers. It is responsible for ensuring that service performance is monitored, measured, and reported; and meets business requirements and agreements
- Component Capacity Management
  - This focus area is the management of the performance, utilization, and capacity of individual technical components possessing finite resources

Includes

- ◆ All aspects of the Performance Management discipline
- ◆ Interfacing with Demand Management on Service Demand Forecasts

[29] ITIL V3 Glossary

- Component capacity management (both as it affects in-house service operations and with consideration of impacts to and requirements upon service partners)
- High-level service capacity monitoring
- Determining the requirements for space and other facilities that will result from capacity proposals and plans

Excludes

- Low-level system capacity monitoring (Service Execution)
- Generalized human resource management (Workforce Management)
- Designing and implementing the facilities needed to support capacity plans (Facilities 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.”[30]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[31]
  - UC: “A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.”[32]

  These agreements can be in a draft or finalized status.

- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and

[30] ITIL V3 Glossary
[31] ITIL V3 Glossary
[32] ITIL V3 Glossary

required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.

- 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.”[33]

Inputs

- 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.

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

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

- Configuration Information (From: A5 A54 A544)

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

- Change Information (From: A5 A51 A518)

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

- 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.

- 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.

- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

- 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.

[33] ITIL V3 Glossary

- 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 Level Package (From: A2 A25 A255)

  Details of the expected implications to the service utility and warranty which will result from agreement with the relevant business units on the demand management approaches under which the service will be provided. ITIL definition: "A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular Pattern of Business Activity."[34]

- 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."[35]

Outputs

- Capacity Reports (To: A256 A744)

  Information about the results and outcomes observed and achieved relating to all aspects of capacity. Reports include:

  - Performance and capacity results
  - Workload analysis
  - Forecasts and predictions

- 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 Resilience Directives (To: A62 A622 A623 A63 A632)

  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.

- Capacity Plan (To: A742 A743 A744 A75 A752)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions

Activities

This process is composed of these activities:

- A741 Establish Capacity Management Framework
- A742 Model and Size Capacity Requirements
- A743 Monitor, Analyze and Report Capacity Usage
- A744 Supervise Tuning and Capacity Delivery
- A745 Produce and Maintain Capacity Plan
- A746 Evaluate Capacity Management Performance

[34] ITIL V3 Glossary
[35] ITIL V3 Glossary

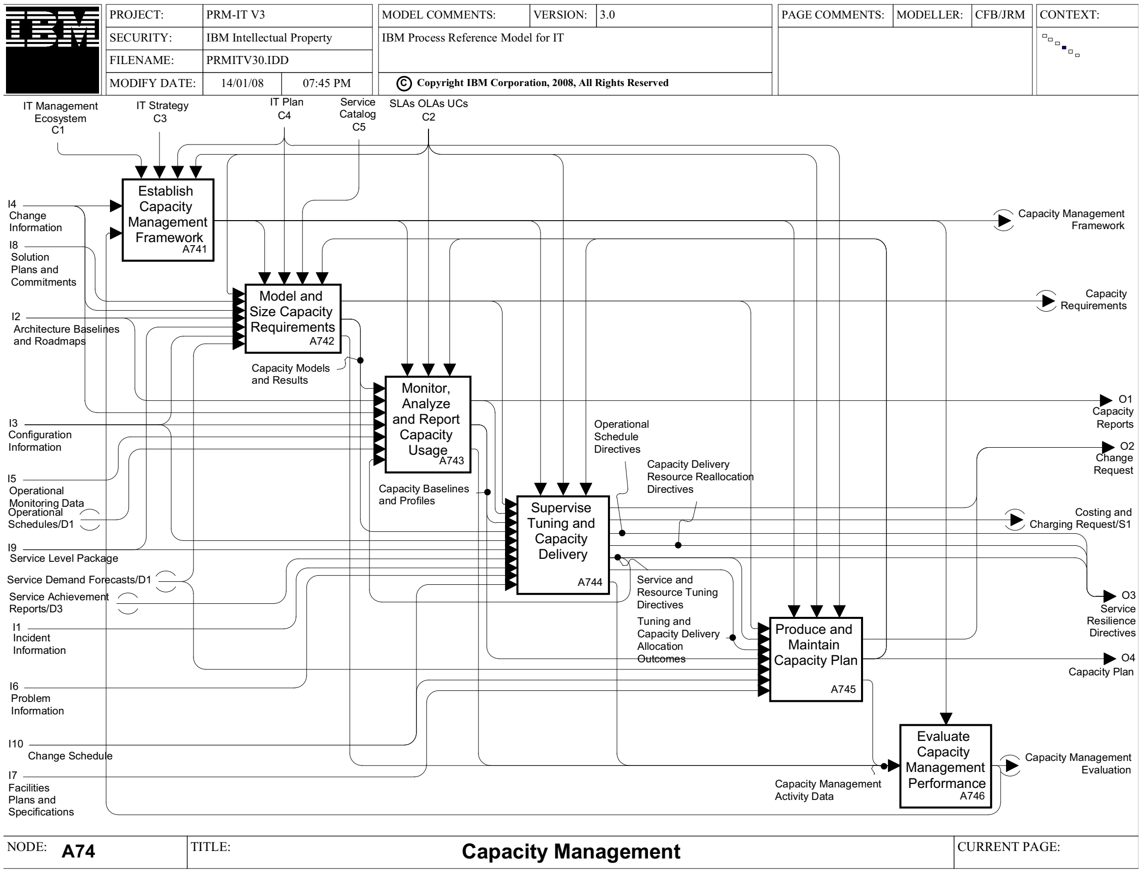

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS: IBM Process Reference Model for IT
VERSION: 3.0
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER: CFB/JRM
CONTEXT:
IT Management Ecosystem C1
IT Strategy C3
IT Plan C4
Service Catalog C5
SLAs OLAs UCs C2
I4 Change Information
I8 Solution Plans and Commitments
I2 Architecture Baselines and Roadmaps
I3 Configuration Information
I5 Operational Monitoring Data
Operational Schedules/D1
I9 Service Level Package
Service Demand Forecasts/D1
Service Achievement Reports/D3
I1 Incident Information
I6 Problem Information
I10 Change Schedule
I7 Facilities Plans and Specifications
Establish Capacity Management Framework A741
Model and Size Capacity Requirements A742
Capacity Models and Results
Monitor, Analyze and Report Capacity Usage A743
Capacity Baselines and Profiles
Supervise Tuning and Capacity Delivery A744
Operational Schedule Directives
Capacity Delivery Resource Reallocation Directives
Service and Resource Tuning Directives
Tuning and Capacity Delivery Allocation Outcomes
Produce and Maintain Capacity Plan A745
Evaluate Capacity Management Performance A746
Capacity Management Activity Data
Capacity Management Framework
Capacity Requirements
O1 Capacity Reports
O2 Change Request
Costing and Charging Request/S1
O3 Service Resilience Directives
O4 Capacity Plan
Capacity Management Evaluation
NODE: A74
TITLE: Capacity Management
CURRENT PAGE:

Figure 5. A74 Capacity Management

[A741] Establish Capacity Management Framework

Description

Based on the business, IT strategy, architectural models and guidelines, a framework for Capacity Management has to be developed.

Some particular items for Capacity Management are:

- Identify the IT resources that will provide the Performance and Capacity services. If a centralized, dedicated team is required and not already in place, then it must be formed by pooling labor fragments from more general IT service support groups.
- Training is a critical step for establishing performance and capacity services due to constant technology change, key linkages with business directions, and the need for good communication and project management skills.
- Establish the basis for a capacity database to contain the business, technical, services and resource information related to capacity. This involves tool selection and deployment, and the establishment of data management for the performance and capacity data. It also involves specifying the data model for a Capacity Management Information System.
  - Defined by ITIL as: “A virtual repository of all Capacity Management data, usually stored in multiple physical locations.” [36]

[36] ITIL V3 Glossary

- Determination of appropriate SLAs and SLRs with the business is required. Establishment of reports against those SLAs and SLRs is required. Definition of IT services to meet the SLAs and SLRs is also required with estimated financial impacts for labor and IT resources.
- Formal linkage with the processes and tools for Incident, Problem, Change, and Release Management, and the Service Desk need to be established. This, too, includes the creation of templates and models for each.

The establishment of the process framework also includes the continuous improvement of Capacity Management. For example, this includes the consideration of the Capacity 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 Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.
- IT Plan (From: A3 A36 A365)

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

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

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[37]
  - 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.”[38]
  - 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

[37] ITIL V3 Glossary

[38] ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[39]

These agreements can be in a draft or finalized status.

Inputs

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.
- Capacity Management Evaluation (From: A746)

  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

- Capacity Management Framework (To: A742 A743 A744 A745 A746)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.

[A742] Model and Size Capacity Requirements

Description

Modeling involves performance and capacity prediction through estimation, trend analysis, analytical modeling, simulation modeling and benchmarking. Modeling can be performed for all or any layer of the IT solution including the business, application and technology infrastructure.

Application sizing is a technique that predicts the service level requirements for response times, throughput, and batch elapsed times. It also predicts resource consumption and cost implications for new or changed applications. It predicts the effect on other interfacing applications. It is performed at the beginning of the solution life cycle and continues through the development, testing and implementation phases. Application sizing has a strong correlation with performance engineering.

Performance engineering is a technique that focuses on the assessment, establishment, and integration of performance planning processes and performance engineering methods within the development life cycle and implementation of prepackaged software. Performance engineering can aid in planning for effective use of existing resources, making informed equipment purchase decisions, and addressing potential performance risks and exposures more quickly. To improve strategic planning and reduce development costs, performance engineering methods and practices can be incorporated into the application development and business planning processes.

Understanding application design implications, system requirements, capabilities and costs early in the application development process improves project planning to help ensure success. Using these processes also helps your staff continually improve system performance, reduce costs, and increase productivity and user satisfaction.

Modeling and sizing are used to determine performance and capacity requirements. These requirements are met by the formulation and implementation of policies. Establishing and maintaining Performance and Capacity Management policies involves administration of pools of specific computing resources by managing policies for how resources are reserved, whether overbooking is allowed, how resources are monitored, and so forth. Resource-specific policies

[39] ITIL V3 Glossary

depend on the characteristics that are associated with particular resource types. For example, storage systems have different characteristics (space allocated, striping, access control) than networks (bandwidth allocation, packet loss rate). A policy framework provides a general, formalized way of controlling such customization and variability within a system through the use of policies.

Controls

- Capacity Management Framework (From: A741)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.
- 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.”[40]
- Capacity Plan (From: A74 A745)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions

Inputs

- 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

[40] ITIL V3 Glossary

responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers."[41]

- 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."[42]
- 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."[43]

These agreements can be in a draft or finalized status.

- 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)

  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.

- 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.

- Service Level Package (From: A2 A25 A255)

  Details of the expected implications to the service utility and warranty which will result from agreement with the relevant business units on the demand management approaches under which the service will be provided. ITIL definition: "A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular Pattern of Business Activity."[44]

- 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 Demand Forecasts (From: A25 A254)

  Agreed predictions of the IT service demand that will be driven if the expected level of business activity occurs. They are usually arranged by periods against a standard calendar.

Outputs

- Capacity Requirements (To: A744 A745)

  Detailed forecasts of the IT resource capacity needed to satisfy projected workloads and service level commitments while maintaining acceptable utilization and load factors.

  For example, they can include: CPU processing power, storage space, and network bandwidth.

[41] ITIL V3 Glossary
[42] ITIL V3 Glossary
[43] ITIL V3 Glossary
[44] ITIL V3 Glossary

- Capacity Models and Results (To: A743 A744)

  Qualitative and quantitative algorithms and projections used to track and predict IT resource capacity and usage patterns.
- Capacity Management Activity Data (To: A746)

  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.

[A743] Monitor, Analyze and Report Capacity Usage

Description

Monitors should be established on all the components and for each of the services. The data should be analyzed using, wherever possible, expert systems to compare usage levels against thresholds. The results of the analysis should be included in reports, and recommendations made as appropriate.

There is a fundamental level of data collection and reporting necessary in any environment before capacity and performance services can be established.

Monitors and Data Collection and Reporting suites might be required at many levels, including but not limited to, the operating system, the database, the transaction processor, middleware, network, Web Services, and end-to-end (user) experience.

Controls

- Capacity Management Framework (From: A741)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.
- SLAs, OLAs, UCs (From: A2 A24 A243)

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

  ITIL definition of these terms:

  - SLA: “An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.”[45]
  - OLA: “An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.”[46]

[45] ITIL V3 Glossary

[46] 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.”[47]

  These agreements can be in a draft or finalized status.

- Capacity Plan (From: A74 A745)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions

Inputs

- Capacity Models and Results (From: A742)

  Qualitative and quantitative algorithms and projections used to track and predict IT resource capacity and usage patterns.

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

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

- Change 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.

- 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.

- 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 and Resource Tuning Directives (From: A744)

  Ranges from traditional performance tuning through capacity and workload allocation adjustments.

Outputs

- Capacity Reports (To: A256 A744)

  Information about the results and outcomes observed and achieved relating to all aspects of capacity. Reports include:

  - Performance and capacity results
  - Workload analysis

[47] ITIL V3 Glossary

- Forecasts and predictions (To: A254 A255 A744 A745)Capacity Baselines and Profiles

  Collective representations of current (and projected) capacity for selected groups of assets and resources, as well as patterns of consumption by various consumers.

- Capacity Management Activity Data (To: A746)

  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.

[A744] Supervise Tuning and Capacity Delivery

Description

Outputs from monitoring, analyzing, and reporting activities are examined and actions to tune individual resources or to re-balance the available capacity are planned and initiated through Change and Release Management. They can also be performed through the Service Desk in the case of simple requests to other support groups or self-help for users. Some recommendations might involve changes in the way that the users use the IT systems. This can include simple recommendations, like moving discretionary workloads to off-peak periods or performing a business function using a more efficient IT service path. Other changes can take the form of balancing services, changing concurrency levels, and adding or removing resources. The cycle then begins again, monitoring any changes made to ensure they have had a beneficial effect and collecting the data for the next day, week, or month.

Service and resource tuning enables effective utilization of IT resources by identifying inefficient performance, excess or insufficient capacity, and making recommendations for optimization. It can balance the need to maintain service while reducing capacity capability to reduce the cost of service.

Understanding the combined performance impact of various components within a complex infrastructure is needed to accurately differentiate symptoms from actual problems. This level of understanding provides the most accurate baseline for future planning. Analysis and tuning can reduce support costs by identifying performance and availability problems, often before they impact your business operations or users. Using this information, decisions can be made to better allocate resources to those areas with the highest business priority.

Recommendations can be made to improve the performance of off-the-shelf applications or unique in-house business applications.

This activity examines the monitored workload demand for servers, middleware, and applications under management. It can sense if performance has degraded and determine what actions need to be taken, either by provisioning and configuring servers, operating systems, middleware, applications, storage, and network devices.

It can be reactive in response to unpredictable business activity. For example, the existing infrastructure provisioning is inadequate relative to increased demand. It can also be done reactively, if a dependent IT infrastructure component is faulty or not working to its expected performance specification. Based on examining performance of resources over time, it can choose to adjust thresholds and warning levels.

The activity can be performed proactively. For example, workload policies are enforced to limit or increase the amount of resources consumed by a particular application or business function. Limitations and constraints can be applied to contain IT processing costs or differentiate the level of service received by one business function over another. Increases in capacity capability can be applied to manage unexpected increases in workload demand.

In summary, this activity makes decisions and performs or requests actions that will result in a better match between resource supply and demand.

Increasingly, the management of resource demand is being automated or semi-automated. Typically, workloads to be managed are expressed in a technology independent manner or virtualized for subsequent mapping onto a physical IT infrastructure. The tools that manage resource demand in this way are said to be performing orchestration or choreography.

Controls

- Capacity Management Framework (From: A741)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.

- 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.”[48]
  - 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.”[49]
  - 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.”[50]

  These agreements can be in a draft or finalized status.

- Capacity Plan (From: A74 A745)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions.

[48] ITIL V3 Glossary
[49] ITIL V3 Glossary
[50] ITIL V3 Glossary

Inputs

- Capacity Requirements (From: A742)

  Detailed forecasts of the IT resource capacity needed to satisfy projected workloads and service level commitments while maintaining acceptable utilization and load factors.

  For example, they can include: CPU processing power, storage space, and network bandwidth.
- Capacity Reports (From: A74 A743)

  Information about the results and outcomes observed and achieved relating to all aspects of capacity. Reports include:

  - Performance and capacity results
  - Workload analysis
  - Forecasts and predictions
- Capacity Baselines and Profiles (From: A743)

  Collective representations of current (and projected) capacity for selected groups of assets and resources, as well as patterns of consumption by various consumers.
- Capacity Models and Results (From: A742)

  Qualitative and quantitative algorithms and projections used to track and predict IT resource capacity and usage patterns.
- 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 Level Package (From: A2 A25 A255)

  Details of the expected implications to the service utility and warranty which will result from agreement with the relevant business units on the demand management approaches under which the service will be provided. ITIL definition: “A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular Pattern of Business Activity.” [51]
- Service Achievement Reports (From: A24 A244)

  One or more reports about how well the service levels have been achieved and which compare IT's actual service level results achieved against the service level standards and any specific service level targets negotiated with customers. The reports can include details of service impacts – both directly measured and an assessment of business impact. Some sections will be for customer distribution and others can be for service provider receipt only.
- 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 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

[51] ITIL V3 Glossary

Change, even though it also contains information about Changes that have already been implemented."[52]

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.
- Costing and Charging Request (To: A833)

  An inquiry about (or an estimate of) the cost or charge related to a particular IT service or cluster of services.
- Operational Schedule Directives

  Desired changes and adjustments to operational schedules, used to optimize the workload throughput or other characteristic within a finite capacity. Sometimes a part of a general Service Resilience Directive.
- Capacity Delivery Resource Reallocation Directives

  Desired changes and adjustments to resource allocations for the purpose of optimizing available capacity against demand. Sometimes a part of a general Service Resilience Directive.
- Service and Resource Tuning Directives (To: A256 A743 A745)

  Ranges from traditional performance tuning through capacity and workload allocation adjustments.
- Tuning and Capacity Delivery Allocation Outcomes (To: A745)

  The results of tuning and capacity delivery allocation activities upon balancing resource supply with workload demand. Some actions will be considered sufficiently permanent to influence the overall capacity plan.
- Capacity Management Activity Data (To: A746)

  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.

[A745] Produce and Maintain Capacity Plan

Description

The objective of this activity is to develop, maintain, test and revise alternative approaches in satisfying various enterprise-shared resource requirements. It delivers the capacity plan that addresses the customer's resource requirements. This plan is configurable, meets performance expectations, and has the required commitment to implement.

The inputs to this activity are forecast assumptions, forecast projections, and subject matter expert recommendations. The controls for this activity are financial constraints, hardware constraints, performance policies, resource standards and definitions, and strategy and direction. The deliverables from this activity are the agreed capacity plan, alternative solutions, and an optimized resource solution.

The Capacity Plan will detail existing usage of critical IT resources under management. Typically, for servers this involves reporting and trend analysis for CPU, I/O, memory, storage, and the network interfaces. The Capacity Plan can also include correlation of IT resource usage to IT

[52] ITIL V3 Glossary

applications (services) and business usage patterns. Similarly, planned business activity and IT application changes and deployments might be factored into forecasts for IT resource requirements.

Controls

- Capacity Management Framework (From: A741)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.

- 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.”[53]
  - 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.”[54]
  - 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.”[55]

  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

- Capacity Requirements (From: A742)

  Detailed forecasts of the IT resource capacity needed to satisfy projected workloads and service level commitments while maintaining acceptable utilization and load factors.

  For example, they can include: CPU processing power, storage space, and network bandwidth.

[53] ITIL V3 Glossary
[54] ITIL V3 Glossary
[55] ITIL V3 Glossary

- Service and Resource Tuning Directives (From: A744)

  Ranges from traditional performance tuning through capacity and workload allocation adjustments.
- Tuning and Capacity Delivery Allocation Outcomes (From: A744)

  The results of tuning and capacity delivery allocation activities upon balancing resource supply with workload demand. Some actions will be considered sufficiently permanent to influence the overall capacity plan.
- Capacity Baselines and Profiles (From: A743)

  Collective representations of current (and projected) capacity for selected groups of assets and resources, as well as patterns of consumption by various consumers.
- Service Demand Forecasts (From: A25 A254)

  Agreed predictions of the IT service demand that will be driven if the expected level of business activity occurs. They are usually arranged by periods against a standard calendar.
- 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.”[56]
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

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.
- Capacity Plan (To: A742 A743 A744 A75 A752)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions
- Capacity Management Activity Data (To: A746)

  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.

[A746] Evaluate Capacity Management Performance

Description

Measurements include the definition, collection of measurements, the analysis, and the review and reporting for Capacity Management. Primarily, the data provides a mechanism to identify and reduce process incidents and problems, propagate best practices as a means for continuous improvement, and to maintain or improve customer satisfaction. Measurement data is also

[56] ITIL V3 Glossary

commonly used to evaluate performance against service level agreement (SLA) objectives and to provide billing and credit information.

There are a number of external factors that can contribute to substandard Capacity Management. However, the measurements are focused on the results of activities within the scope of this process.

The effectiveness and efficiency measurements for Capacity Management are described. Note that the order of the measurements listed does not necessarily indicate their order of importance.

- The percentage of IT resources under management for which a standard, pre-defined set of performance and capacity data is routinely collected, summarized and reported on for trends and exceptions.
- The timely production and distribution of accurate standard reports. In order to assure the timely delivery of reports, report timeliness is calculated as a percentage of standard reports delivered on or before the commitment date.
- Capacity Planner Productivity: Work units per analyst where work units are normalized measurements of workload taking into account various server support variables like maturity, complexity, and seasonal variability.
- Number of escalations per month, raised by Incident or Problem Management. Escalations are defined as *severity one* incidents where the root cause has been determined to be within the scope of Capacity Management.
- Proactive Capacity Planning for planning timeliness and accuracy. The capacity plan is accepted and maintained in a timely manner and approved recommendations from the capacity plan for hardware or software upgrades are implemented and validated for efficacy and cost.
- The percentage of performance and capacity service level agreements achieved in a specified period of time.
- The accuracy of tuning benefits predicted.

Controls

- Capacity Management Framework (From: A741)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), information (entities, attributes, relationships) and technology (software, hardware) practices for managing capacity.

Inputs

- Capacity Management Activity Data (From: A742 A743 A744 A745)

  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

- Capacity Management Evaluation (To: A741)

  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.

[A75] Facilities Management

Purpose

The purpose of the Facilities Management process is to create and maintain a physical environment that houses IT resources and to optimize the capabilities and cost of that environment.

Definition of Facilities Management: “The Function responsible for managing the physical Environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical Environment, for example power and cooling, building Access Management, and environmental Monitoring”.[57]

Outcomes

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

- The physical environment within which information technology resources perform supports operational needs
- Availability of IT systems is protected from physical threats (including environmental, security, continuity)
- Facility requirements are analyzed, planned for, and met in a timely and cost-effective manner

Scope

Includes

- Physical facilities planning and implementation (physical planning) – space, power, HVAC, physical cables and connectors, physical security implementation, protection (such as sprinklers, halon systems, badge readers, security personnel)
- Physical logistics (receipt, staging, moving)
- Physical environment for all information and communications technology
  - For example, participating in the design of racks and cabling
- Physical access management to IT facilities
- Safety
- Managing incidents concerning facilities, and interfacing with Incident Management when both IT and Facilities components are involved

Excludes

- Asset Management
- Procurement (Supplier Management)
- Business resilience and continuity (Business responsibility, in conjunction with IT Service Continuity Management)
- Corporate facilities (buildings, maintenance, catering, mail delivery, desks, lights) unless associated with a secure data center (Business responsibility)

[57] ITIL V3 Glossary

- Security of corporate facilities, such as office buildings, factories (Business responsibility)
- IT security policies and practices (Security Management)
- Media management (see Data Management) but would include physical transportation and security of media
- Management of suppliers (Supplier Management)

Controls

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

  The records that 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 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.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- 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.”[58]

[58] 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.”[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 Strategy (From: A3 A31 A315)

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

- IT 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 Budget (From: A8 A81 A813)

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

- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.

Inputs

- Capacity Plan (From: A74 A745)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions

- Availability Plan (From: A73 A737)

  A forward-looking plan aimed at improving the overall availability of the IT infrastructure within cost constraints.

- 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).

- 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.

[59] ITIL V3 Glossary
[60] 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.

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

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

- Solution Design (From: A4 A42 A425)

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

- 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]

- Configuration Information (From: A5 A54 A544)

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

- Change Information (From: A5 A51 A518)

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

- IT Service Continuity Plan (From: A76 A764)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.

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.

- 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

- Facilities Plans and Specifications (To: A72 A723 A726 A73 A737 A74 A745 A753 A754 A76 A764)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

[61] ITIL V3 Glossary

Activities

This process is composed of these activities:

- A751 Establish Facilities Management Framework
- A752 Plan Facilities
- A753 Manage Facility Request
- A754 Operate and Maintain Facilities
- A755 Evaluate Facilities Management Performance

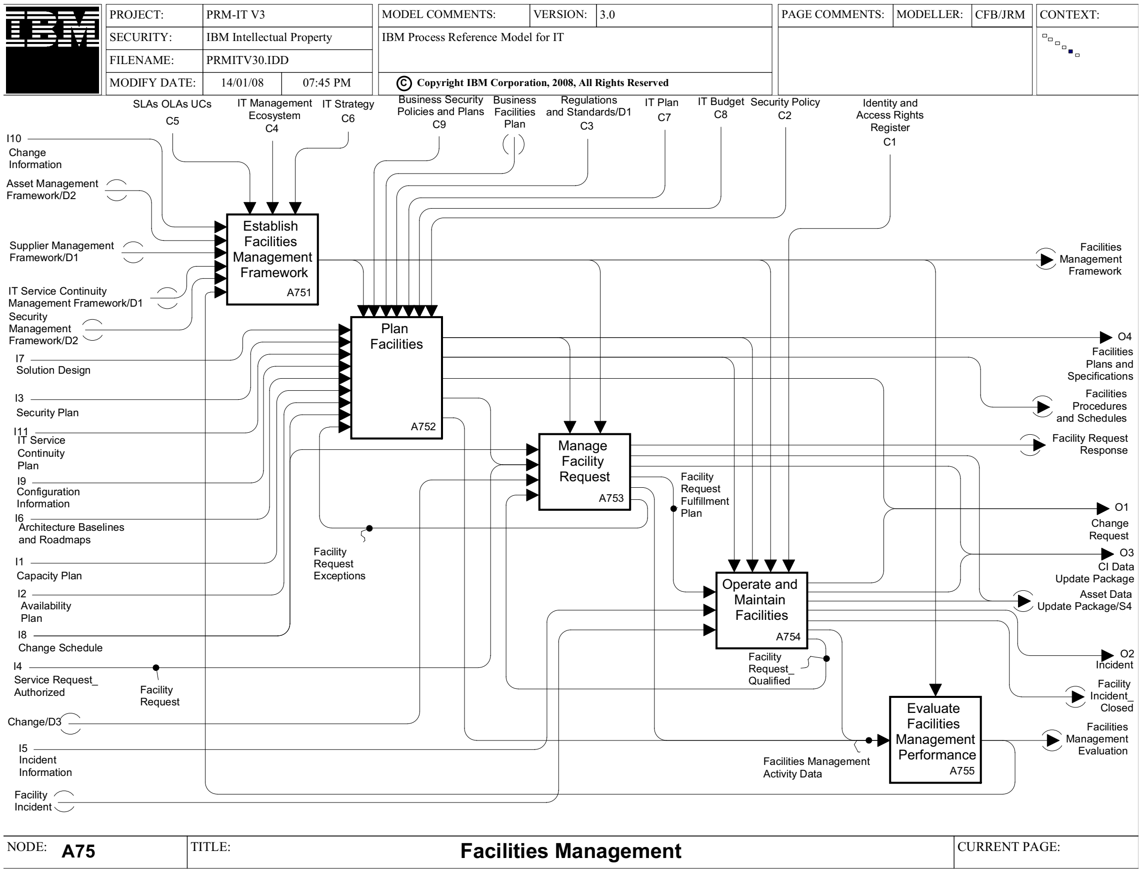

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS: VERSION: 3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS: MODELLER: CFB/JRM
CONTEXT:
SLAs OLAs UCs C5
IT Management Ecosystem C4
IT Strategy C6
Business Security Policies and Plans C9
Business Facilities Plan
Regulations and Standards/D1 C3
IT Plan C7
IT Budget C8
Security Policy C2
Identity and Access Rights Register C1
I10 Change Information
Asset Management Framework/D2
Supplier Management Framework/D1
IT Service Continuity Management Framework/D1
Security Management Framework/D2
I7 Solution Design
I3 Security Plan
I11 IT Service Continuity Plan
I9 Configuration Information
I6 Architecture Baselines and Roadmaps
I1 Capacity Plan
I2 Availability Plan
I8 Change Schedule
I4 Service Request_ Authorized
Facility Request
Change/D3
I5 Incident Information
Facility Incident
Establish Facilities Management Framework A751
Plan Facilities A752
Manage Facility Request A753
Operate and Maintain Facilities A754
Evaluate Facilities Management Performance A755
Facility Request Exceptions
Facility Request Fulfillment Plan
Facility Request_ Qualified
Facilities Management Activity Data
Facilities Management Framework
O4 Facilities Plans and Specifications
Facilities Procedures and Schedules
Facility Request Response
O1 Change Request
O3 CI Data Update Package
Asset Data Update Package/S4
O2 Incident
Facility Incident_ Closed
Facilities Management Evaluation
NODE: A75
TITLE: Facilities Management
CURRENT PAGE:

Figure 6. A75 Facilities Management

[A751] Establish Facilities Management Framework

Description

This activity defines and documents the rules, policies, standards, guidelines and practices governing day-to-day IT facility operations. The scope includes managing assets, service levels, suppliers of service (internal and third party), physical security, and IT continuity in accordance with corporate policies and plans.

Controls

- 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.”[62]
  - 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.”[63]
  - 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.”[64]

  These agreements can be in a draft or finalized status.

- 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 Strategy (From: A3 A31 A315)

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

[62] ITIL V3 Glossary
[63] ITIL V3 Glossary
[64] ITIL V3 Glossary

Inputs

- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.
- Asset Management Framework (From: A551)

  The policies, procedures, organizational roles and responsibilities and other information under which the Asset Management process will operate to meet its mission and goals.
- Supplier Management Framework (From: A821)

  The framework that contains all relevant information about the structure of the Supplier Management process, meaning the practices for supplier management and procurement. This includes evaluation criteria for selection and evaluation of suppliers, and relevant systems.
- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.
- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.
- Facilities Management Evaluation (From: A755)

  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

- Facilities Management Framework (To: A752 A753 A754 A755)

  The policies, guidelines, plans, procedures and targets for the workings of the Facilities Management process.

[A752] Plan Facilities

Description

This activity is the ongoing effort to plan new buildings or updates to existing buildings and other facilities so they efficiently provide the physical infrastructure (electric, water, backup power, security, cabling) to support IT service level requirements. This activity should be closely aligned with the business strategy, regulations and standards, as well as IT plans.

Controls

- Facilities Management Framework (From: A751)

  The policies, guidelines, plans, procedures and targets for the workings of the Facilities Management process.
- Business Security Policies and Plans

  This is the overall set of security directives from the business, establishing the context for protection of business assets and information. It is often known as an *Enterprise Security Program*.

- Business Facilities Plan

  The plan, established by the Business, describing the quantity, locations, and other Facility items that enable it to operate.
- Regulations and Standards
- External official rules (typically driven by government) that call for business compliance, as well as established good practice standards from formal and informal bodies. Includes:
  - Generally accepted accounting principles
  - Legal requirements, such as Sarbanes-Oxley and its COSO (Framework for Financial Management)
- 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 Budget (From: A8 A81 A813)

  The planned IT funding broken down in relevant ways, such as activities and milestones per period, to reflect the contents of the IT plan.
- 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).
- IT Service Continuity Plan (From: A76 A764)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.
- 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.
- 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.
- Capacity Plan (From: A74 A745)

  The approach that will be taken to satisfy resource requirements. The plan is configurable, meets performance expectations and has the required commitment to implement. It includes:

  - SLA recommendations
  - Threshold and alarm definitions
- Availability Plan (From: A73 A737)

  A forward-looking plan aimed at improving the overall availability of the IT infrastructure within cost constraints.
- 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."[65]
- Facility Request Exceptions (From: A753)

  This is an ad hoc request that does not conform to the current plans, but is within the overall remit of the facility framework. It can potentially be addressed by some additional facility planning.

Outputs

- Facilities Plans and Specifications (To: A72 A723 A726 A73 A737 A74 A745 A753 A754 A76 A764)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- Facilities Procedures and Schedules (To: A754)

  Documentation on facilities procedures, facilities availability, and use of facility infrastructure for IT and the user community. This information is available to Knowledge Management, for it to determine which parts (if any) are needed to be available to the IT processes.
- 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.
- Facility Request (To: A753)

  A request for Facility changes that conform to the framework or the plans for the facility.
- Facilities Management Activity Data (To: A755)

  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.

[A753] Manage Facility Request

Description

This activity evaluates facility requests, formulates the plans on how they will be fulfilled, and manages the request through completion.

Controls

- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.

[65] ITIL V3 Glossary

- Facilities Management Framework (From: A751)

  The policies, guidelines, plans, procedures and targets for the workings of the Facilities Management process.

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.”[66]

- Facility Request (From: A752)

  A request for Facility changes that conform to the framework or the plans for the facility.

- Change (From: A51 A515)

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

- Facility Request_ Qualified (From: A754)

  A need for a facility request to be re-planned as a result of an operation or maintenance activity producing a result out of line with the plan.

Outputs

- Facility Request Response

  The fulfillment of the Facility Request and information about it, including:

  - Description of the request
  - Notification to the requestor as to how the request was addressed
  - Updates to CI information and asset information

- 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

- Facility Request Fulfillment Plan (To: A754)

  The plan (instructions, specifications) for the fulfillment of the facility request using normal facility operation or maintenance.

- Facilities Management Activity Data (To: A755)

  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.

[66] ITIL V3 Glossary

- Facility Request Exceptions (To: A752)

  This is an ad hoc request that does not conform to the current plans, but is within the overall remit of the facility framework. It can potentially be addressed by some additional facility planning.

[A754] Operate and Maintain Facilities

Description

This activity addresses the tasks that perform the work required to achieve efficient day-to-day running of the IT facilities, as well as raising requests for new facility elements and considering facilities-related incident information.

Controls

- Facilities Procedures and Schedules (From: A752)

  Documentation on facilities procedures, facilities availability, and use of facility infrastructure for IT and the user community. This information is available to Knowledge Management, for it to determine which parts (if any) are needed to be available to the IT processes.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- Facilities Management Framework (From: A751)

  The policies, guidelines, plans, procedures and targets for the workings of the Facilities Management process.
- Identity and Access Rights Register (From: A6 A67 A673 A674)

  The records that 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).

Inputs

- Facility Request Fulfillment Plan (From: A753)

  The plan (instructions, specifications) for the fulfillment of the facility request using normal facility operation or maintenance.
- 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.
- Facility Incident

  An external event resulting in a real or suspected failure of one or many components of the facility, and the related notification and information about the incident.

  - Facility incidents might be handled separately (for example, by the business) from the IT Incident Management process

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.
- 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
- 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.
- 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.
- Facility Incident_ Closed

  Information about the facility incident life cycle and outcome, including:
  - Notification to the requestor that the request was addressed
  - Feedback to any relevant IT processes, such as supplier management, workforce management, financial management
- Facilities Management Activity Data (To: A755)

  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.
- Facility Request_ Qualified (To: A753)

  A need for a facility request to be re-planned as a result of an operation or maintenance activity producing a result out of line with the plan.

[A755] Evaluate Facilities Management Performance

Description

This is the continuing activity of monitoring the current IT Facilities Management Performance. It utilizes established facilities measures (as defined by the process framework). This activity is conducted in order to make key measurements of the health of the facility management system, as well as factors other than measurements, that might indicate a need for change in the facility management system.

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, and 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.

- Facilities Management FrameworkControls (From: A751)

  The policies, guidelines, plans, procedures and targets for the workings of the Facilities Management process.

Inputs

- Facilities Management Activity Data (From: A752 A753 A754)

  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

- Facilities Management Evaluation (To: A751)

  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.

[A76] IT Service Continuity Management

Purpose

The purpose of the Service Continuity Management process is to ensure that agreed IT services will support business requirements in the event of a disruption to the business, based on the committed recovery schedule.

Definition of IT Service Continuity Management: “The Process responsible for managing Risks that could seriously impact IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.”[67]

Outcomes

As a result of the successful implementation of the IT Service Continuity Management process:

- A set of IT Service Continuity and IT Recovery plans are created, maintained, and tested that support the organization’s overall Business Continuity Plans
- Business continuity targets can be met through the recovery of agreed IT services and technical facilities to agreed time scales, under Change Management control
- Regulatory requirements for IT service continuity are met
- Business vitality and functions are maintained at agreed levels

Scope

The process fulfils its mission through risk reduction measures, controlled recovery options, and restoration facilities.

Includes

- Service capability for prioritized, critical business processes, and their attendant support requirements. Examples include:
  - IT application services
  - Organizational procedures
  - Consideration of facilities
  - Consideration of IT Services provided by business partners
- Specification of service continuity solutions
- Definition of circumstances and thresholds for continuity invocation
- Contributing to proactive prevention of IT disruptions (by identifying and analyzing risks, and sharing the analysis)
- Control of continuity solution invocation in the event of disruption
- Testing of the continuity solution

Excludes

- Normal operational fluctuations (Service Execution, Event Management)
- Minor technical faults that are covered by Incident Management

[67] ITIL V3 Glossary

- Deliberate business strategy changes and long term risks such as business diversification or restructuring (IT Strategy)
- Responsibility for identification and prioritization of critical business processes (performed in a business impact analysis by the Business Continuity Management process: outside the scope of this model)
- Development and implementation of service continuity solutions (once agreed by Portfolio Management, these solutions are treated as any other solution through Realization and Transition)
- Contractual arrangements with third parties (Supplier Management)

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).
- 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.”[68]
- 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.
- 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.

[68] 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.”[69]
- 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.”[70]
- 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.”[71]

These agreements can be in a draft or finalized status.

- IT Strategy (From: A3 A31 A315)

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

  Known risks, threats and vulnerabilities which exist from other organizations in the same business sector, and environmental risk.
- 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.
- Business Continuity Policies

  Rules and guidelines used to assist in the determination of critical business services, and in the determination of potential risks, threats, and vulnerabilities.

Inputs

- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT 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.
- 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

[69] ITIL V3 Glossary
[70] ITIL V3 Glossary
[71] ITIL V3 Glossary

- 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.

- 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.

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

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

- Solution Design (From: A4 A42 A425)

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

- 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_ 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.

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.

- Service Resilience Directives (To: A62 A622 A623 A63 A632)

  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.

- IT Service Continuity Plan (To: A75 A752 A765 A766)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.

Activities

This process is composed of these activities:

- A761 Establish IT Service Continuity Management Framework
- A762 Identify Business Service Continuity Requirements
- A763 Create and Maintain IT Service Continuity Strategy
- A764 Create and Maintain IT Service Continuity Plan
- A765 Prepare IT Service Continuity Capability

- A766 Execute IT Service Continuity Plan
- A767 Evaluate IT Service Continuity Management Performance

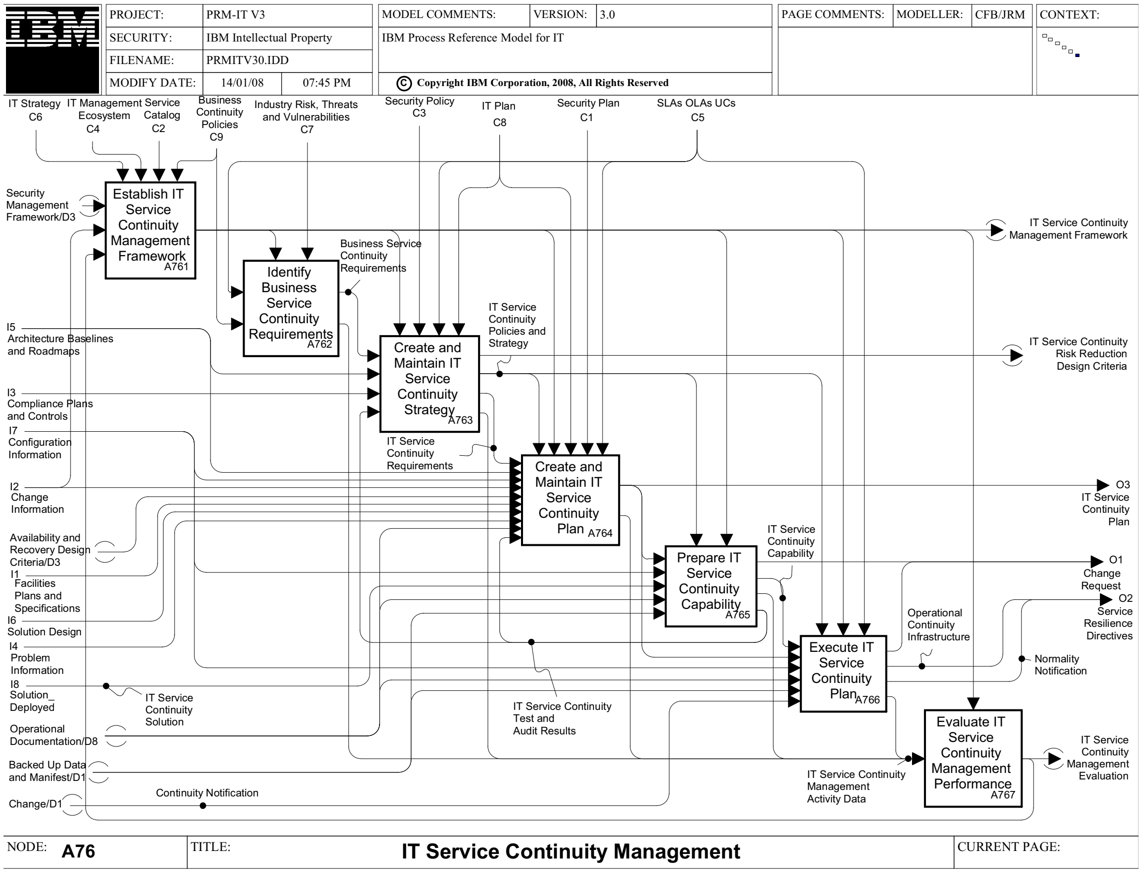

PROJECT: PRM-IT V3
SECURITY: IBM Intellectual Property
FILENAME: PRMITV30.IDD
MODIFY DATE: 14/01/08 07:45 PM
MODEL COMMENTS:
VERSION: 3.0
IBM Process Reference Model for IT
© Copyright IBM Corporation, 2008, All Rights Reserved
PAGE COMMENTS:
MODELLER: CFB/JRM
CONTEXT:
IT Strategy C6
IT Management Ecosystem C4
Service Catalog C2
Business Continuity Policies C9
Industry Risk, Threats and Vulnerabilities C7
Security Policy C3
IT Plan C8
Security Plan C1
SLAs OLAs UCs C5
Security Management Framework/D3
Establish IT Service Continuity Management Framework A761
IT Service Continuity Management Framework
Identify Business Service Continuity Requirements A762
Business Service Continuity Requirements
I5 Architecture Baselines and Roadmaps
I3 Compliance Plans and Controls
I7 Configuration Information
Create and Maintain IT Service Continuity Strategy A763
IT Service Continuity Policies and Strategy
IT Service Continuity Risk Reduction Design Criteria
IT Service Continuity Requirements
I2 Change Information
Create and Maintain IT Service Continuity Plan A764
O3 IT Service Continuity Plan
Availability and Recovery Design Criteria/D3
I1 Facilities Plans and Specifications
I6 Solution Design
I4 Problem Information
I8 Solution_ Deployed
IT Service Continuity Capability
Prepare IT Service Continuity Capability A765
O1 Change Request
O2 Service Resilience Directives
Operational Continuity Infrastructure
Normality Notification
Execute IT Service Continuity Plan A766
IT Service Continuity Solution
IT Service Continuity Test and Audit Results
Evaluate IT Service Continuity Management Performance A767
IT Service Continuity Management Evaluation
Operational Documentation/D8
Backed Up Data and Manifest/D1
IT Service Continuity Management Activity Data
Continuity Notification
Change/D1
NODE: A76
TITLE: IT Service Continuity Management
CURRENT PAGE:

Figure 7. A76 IT Service Continuity Management

[A761] Establish IT Service Continuity Management Framework

Description

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

- Understanding and developing the business strategy and legal and self-imposed regulations with regard to service continuity
- Establishing the framework for Service Continuity Management by defining and implementing practices and systems that support process activities
- Determining skill requirements for the staff and assigning staff based on these systems

Finally, the structure and process of IT Service Continuity Management including continuity responsibilities have to be communicated to the process users.

The establishment of the process framework also includes the continuous improvement of IT Service Continuity Management. For example, the consideration of the IT Service Continuity process evaluation and the implementation of recommended improvement actions.

Controls

- IT Strategy (From: A3 A31 A315)

  A consolidated statement of IT initiatives. Includes a summary of changes to IT capabilities and a summary of each strategic IT initiative. Also includes a statement of planned and required changes to the IT Portfolio and IT Plan. The IT Sourcing Strategy would be included.
- IT Management Ecosystem (From: A1)

  To paraphrase a dictionary definition: the complex of management system elements, their physical implementation, and all their interrelationships in the unit of space that is the domain of the IT function. Its fundamental purpose is to provide an environment that is supportive of the carrying out of all of the IT activities defined elsewhere in this model.
- 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.”[72]
- Business Continuity Policies

  Rules and guidelines used to assist in the determination of critical business services, and in the determination of potential risks, threats, and vulnerabilities.

Inputs

- Security Management Framework (From: A721)

  The conceptional structure describing the strategic (vision, mission, value proposition), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs), and technology (software, hardware) practices for managing security.
- 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.
- IT Service Continuity Management Evaluation (From: A767)

  Assessment results for the IT Service Continuity Management process and it activities, including process performance metrics and the identification of potential process improvement items.

Outputs

- IT Service Continuity Management Framework (To: A751 A762 A763 A764 A765 A766 A767)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.

[72] ITIL V3 Glossary

[A762] Identify Business Service Continuity Requirements

Description

This activity identifies those business services which are critical for the ability of an organization to survive. In carrying out the activities associated with the identification of these services, relevant IT support processes, such as Problem Management, are also identified as these too form a service in supporting the business.

The activity continues with an impact analysis that identifies what will happen in the result of the loss, or degradation, of one or more of those critical business services.

Further, an assessment is made to identify risks and determine the vulnerability of each business service.

This activity culminates in a set of Business Service Continuity requirements.

Controls

- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.
- Industry Risk Threats and Vulnerabilities

  Known risks, threats and vulnerabilities which exist from other organizations in the same business sector, and environmental risk.

Inputs

- 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.”[73]
  - 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.”[74]
  - 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

[73] ITIL V3 Glossary

[74] ITIL V3 Glossary

Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA."[75]

These agreements can be in a draft or finalized status.

- Business Continuity Policies

  Rules and guidelines used to assist in the determination of critical business services, and in the determination of potential risks, threats, and vulnerabilities.

Outputs

- Business Service Continuity Requirements (To: A763)

  The results of a business impact analysis, with identified risks, threats, and vulnerabilities.
- IT Service Continuity Management Activity Data (To: A767)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.

[A763] Create and Maintain IT Service Continuity Strategy

Description

This activity is responsible for identifying risk reduction measures for the business services identified, and to establish what countermeasures and recovery options exist to support these services should they be adversely affected.

It takes into account the types of risks that might be encountered, and the potential costs involved for each recovery option.

The result of this activity is an agreed IT Service Continuity Strategy and a set of IT service continuity requirements.

Controls

- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.
- 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.
- 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.

[75] 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.”[76]
- 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.”[77]
- 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.”[78]

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

- ■ Business Service Continuity Requirements (From: A762)

  The results of a Business Impact Analysis, with identified risks, threats, and vulnerabilities.
- ■ 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.
- ■ 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 Service Continuity Test and Audit Results (From: A765)

  Data (or reports) detailing the success or failure of a planned, or unplanned, test of the IT Service Continuity Plan.

Outputs

- ■ IT Service Continuity Risk Reduction Design Criteria

  Identification of approaches which, if adopted in the design of the solution and in its implementation as a service, would reduce overall continuity risk.

[76] ITIL V3 Glossary

[77] ITIL V3 Glossary

[78] ITIL V3 Glossary

- IT Service Continuity Policies and Strategy (To: A764 A765 A766)

  The guiding statements which direct the IT Service Continuity preparations, maintenance of readiness and actual invocation. For example, they include rules that must be adhered to in the event of either a test or an invocation of the IT Service Continuity Plan.
- IT Service Continuity Requirements (To: A764)

  Includes details of prioritization of Capacity, Availability, and other Service Level items that must be satisfied by the IT Service Continuity Capability.
- IT Service Continuity Management Activity Data (To: A767)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.

[A764] Create and Maintain IT Service Continuity Plan

Description

This process is responsible for identifying:

- The infrastructure (people, processes, technology) necessary to support the required services in the event that the continuity is invoked.
- The actions that would then be taken to result in successful invocation of the IT Service Continuity Plan.

It is also responsible for the ongoing maintenance of the plan and takes into account changes to critical business services and changes to the infrastructure that these business processes use. This process culminates in the creation of the IT Service Continuity Plan, which is then placed under change control and also forms part of the Business Continuity Plan.

Controls

- IT Service Continuity Policies and Strategy (From: A763)

  The guiding statements which direct the IT Service Continuity preparations, maintenance of readiness and actual invocation. For example, they include rules that must be adhered to in the event of either a test or an invocation of the IT Service Continuity Plan.
- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.
- 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 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).
- 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."[79]
- 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."[80]
- 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."[81]

These agreements can be in a draft or finalized status.

Inputs

- IT Service Continuity Requirements (From: A763)

  Includes details of prioritization of Capacity, Availability, and other Service Level items that must be satisfied by the IT Service Continuity Capability.
- Architecture Baselines and Roadmaps (From: A3 A33 A334)

  Provides an agreed, published statement of the required architecture at a moment in time. Includes statements to assist in selection and evaluation of appropriate implementations of specified architecture building blocks.
- Configuration Information (From: A5 A54 A544)

  The information on any individual configuration item (CI) or collection of CIs, which is made available using standard reports or to meet individual requests.
- Change Information (From: A5 A51 A518)

  The full scope of information is covered. This could be about an individual detail within a particular change through ad hoc or pre-determined reporting on a set of changes.
- Availability and Recovery Design Criteria (From: A733)

  General solution design principles that enhance service availability and recovery. This information is used to create or update solutions so that they are more resilient.
- Facilities Plans and Specifications (From: A75 A752)

  Specifications, designs and plans for the IT facilities to support the provision of IT service.
- 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.

[79] ITIL V3 Glossary
[80] ITIL V3 Glossary
[81] 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.
- 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.
- IT Service Continuity Test and Audit Results (From: A765)

  Data (or reports) detailing the success or failure of a planned, or unplanned, test of the IT Service Continuity Plan.

Outputs

- IT Service Continuity Plan (To: A75 A752 A765 A766)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.
- IT Service Continuity Management Activity Data (To: A767)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.

[A765] Prepare IT Service Continuity Capability

Description

This process ensures that an invocation of the IT Service Continuity Plan results in the ability to recover and restore required services to a predetermined level, and in a predetermined time frame. It has the responsibility for ensuring that all plans are tested regularly, both on a planned and unplanned basis; that the process passes audit requirements; and that the results from tests are captured and fed back to other processes to ensure that the IT Service Continuity Plan remains fit for purpose.

Controls

- IT Service Continuity Policies and Strategy (From: A763)

  The guiding statements which direct the IT Service Continuity preparations, maintenance of readiness and actual invocation. For example, they include rules that must be adhered to in the event of either a test or an invocation of the IT Service Continuity Plan.
- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.

Inputs

- IT Service Continuity Plan (From: A76 A764)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.
- 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.
- IT Service Continuity Solution

  The technical solution which will provide the infrastructure for continuity testing and invocation.
- 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.
- Backed Up Data and Manifest (From: A635)

  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.

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.
- IT Service Continuity Capability (To: A766)

  The combination of infrastructure and human resources (associated process and organization) which IT can invoke the IT Service Continuity Plan.
- IT Service Continuity Management Activity Data (To: A767)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.
- IT Service Continuity Test and Audit Results (To: A763 A764)

  Data (or reports) detailing the success or failure of a planned, or unplanned, test of the IT Service Continuity Plan.

[A766] Execute IT Service Continuity Plan

Description

This process is responsible for implementing the IT Service Continuity Plan, according to predetermined criteria. It is responsible for maintaining business operations for an unspecified amount of time, and for ensuring a controlled restoration to normal service.

Controls

- IT Service Continuity Policies and Strategy (From: A763)

  The guiding statements which direct the IT Service Continuity preparations, maintenance of readiness and actual invocation. For example, they include rules that must be adhered to in the event of either a test or an invocation of the IT Service Continuity Plan.

- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.

- 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.”[82]
  - 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.”[83]
  - 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.”[84]

  These agreements can be in a draft or finalized status.

Inputs

- IT Service Continuity Capability (From: A765)

  The combination of infrastructure and human resources (associated process and organization) which IT can invoke the IT Service Continuity Plan.

[82] ITIL V3 Glossary
[83] ITIL V3 Glossary
[84] ITIL V3 Glossary

- IT Service Continuity Plan (From: A76 A764)

  A formal, documented plan describing procedures to be adhered to in order to facilitate the recovery and restoration of critical business services. Includes a possible need for new capabilities to meet service continuity requirements.

- 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 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.

- Backed Up Data and Manifest (From: A635)

  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.

- Continuity Notification

  An urgent, formal command to invoke the IT Service Continuity Plan.

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 Continuity Infrastructure

  The IT Service Continuity Solution in live state, ready for delivering the planned level of operational service, and all relevant details about it so that the regular set of processes can perform their work, within the limitations of that continuity solution.

- Normality Notification

  A notification that critical business services have been stabilized to a condition that reflects the new *normal operation*, following a period of operating under continuity status.

- IT Service Continuity Management Activity Data (To: A767)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.

[A767] Evaluate IT Service Continuity Management Performance

Description

This process evaluates the performance of the Service Continuity Management process. It aims to identify areas of the overall process requiring improvement. This means the foundation and interfaces of the process, its activities, their accomplishment, their degree of automation, as well as the roles and responsibilities including the respective skills. Target for evaluations also includes the continuity suppliers and supply items.

The basis for the improvements is the insights and lessons learned from the observations and analysis of activity accomplishments and results.

Controls

- IT Service Continuity Management Framework (From: A761)

  The conceptional structure describing the strategic (vision, mission, value proposition, policies), organizational (organizational mechanisms, roles, accountabilities), process (activities, work flows, inputs, outputs, procedures), information (data model, management reports) and technology (software, hardware) practices for managing IT service continuity.

Inputs

- IT Service Continuity Management Activity Data (From: A762 A763 A764 A765 A766)

  Data resulting from all work carried out by each process activity, used to support the evaluation of the overall IT Service Continuity Management process.

Outputs

- IT Service Continuity Management Evaluation (To: A761)

  Assessment results for the IT Service Continuity Management process and it activities, including process performance metrics and the identification of potential process improvement items.

PRM-IT A7 Node Tree

A7 – RESILIENCE	
A71	**Compliance Management**
A711	Establish Compliance Management Framework
A712	Identify Compliance Requirements
A713	Assess Compliance Requirements
A714	Define Compliance Controls Plan
A715	Implement Compliance Controls
A716	Audit and Report Compliance
A717	Evaluate Compliance Management Performance
A72	**Security Management**
A721	Establish Security Management Framework
A722	Produce and Maintain Security Policy
A723	Analyze Security Threats, Vulnerabilities and Risks
A724	Classify Information Asset Security
A725	Plan and Implement Security Practices
A726	Operate Security Protection Mechanisms
A727	Monitor, Assess, Audit and Report Security
A728	Evaluate Security Management Performance
A73	**Availability Management**
A731	Establish Availability Management Framework
A732	Determine Availability Requirements
A733	Formulate Availability and Recovery Design Criteria
A734	Define and Implement Availability Targets and Related Measures
A735	Monitor, Analyze and Report Availability
A736	Investigate Unavailability
A737	Produce Availability Plan
A738	Evaluate Availability Management Performance
A74	**Capacity Management**
A741	Establish Capacity Management Framework
A742	Model and Size Capacity Requirements
A743	Monitor, Analyze and Report Capacity Usage
A744	Supervise Tuning and Capacity Delivery
A745	Produce and Maintain Capacity Plan
A746	Evaluate Capacity Management Performance
A75	**Facility Management**
A751	Establish Facility Management Framework
A752	Plan Facilities
A753	Manage Facility Request
A754	Operate and Maintain Facilities
A755	Evaluate Facilities Management Performance
A76	**IT Service Continuity Management**

A7 – RESILIENCE	
A761	Establish IT Service Continuity Management Framework
A762	Identify Business Service Continuity Requirements
A763	Create and Maintain IT Service Continuity Strategy
A764	Create and Maintain IT Service Continuity Plan
A765	Prepare IT Service Continuity Capability
A766	Execute IT Service Continuity Plan
A767	Evaluate IT Service Continuity Management Performance

Figure 8. A7 Resilience Node Tree