Excerpt

ITSM Processes of

Service Operation

according to ITIL® 2011

.... the processes ....
.... the tasks ....
.... the roles ....
.... the responsibilities ....
.... the involved parties ....
This ebook is the 4th volume of our series „ITSM Processes according to ITIL® 2011“ based upon the well known ITIL® 2011 Process Library from Dipl.-Ing. Walter Abel Management Consulting. This ebook series describes the processes of IT Service Management in the leading process management tool Signavio Process Editor notated in BPMN 2.0. The content results from the experience of nearly 20 years of practice in successful implementing ITSM projects.

We want to provide a process oriented guide of the complex topic of ITIL® 2011 by this ebook that

- avoids the awful evaluation of necessary processes in the beginning of your IT Service Management project
- provides a completeness check of your planned process model
- shows the internal and external interfaces of IT Service Management

and thus accelerates your projekt remarkably and saves costs also (especially external consulting costs).

The purpose of this ebook is not provision of theoretical knowledge but shows the experience of numerous implementations of process oriented IT Service Management from practice. From the perspective of the ITIL® standard all subtopics have more or less the same priority - practice shows a different picture. We have built our process library described in this publication exactly to practical considerations, practical relevance has the primary focus.

Each process is described by

- its process diagram
- its subprocesses (within interface diagrams)
- its tasks (within process diagrams)
- involved organizational units
- involved roles
- involved IT systems

The glossary at the end of the document outlines detailed descriptions of

- process documents
- involved organizational units
- involved roles
- involved IT systems

and provides checklists to key topics.

And now i wish you a fruitful and interesting reading!

Yours

Dipl.-Ing. Walter Abel
Legal notice

The author does not warrant the success of implementing the knowledge from this publication as this depends on the personal skills of the user. All content of this ebook and the complete ITIL® 2011 Process Library have been carefully researched and developed. In case content of other media are affected wrongfully by this publication the author has to be informed in writing without any prior dissuasion. The author will check the circumstances and rework the respective content in case of reasonable objection. The author is in no way liable for pages reachable via recommended links. For the content of those pages the operator of the respective web page is solely responsible.

This ebook is protected by copyright. You may print this ebook for personal use. Handing over of printouts to third parties is not permitted.

Copyright, trademarks and property rights

„Signavio“ and „Signavio Process Editor“ are trademarks of Signavio GmbH, Goethestraße 2 - 3, D - 10623 Berlin
„ITIL®“ is a registered trademark of the Cabinet Office in Great Britain and other countries

Printing this ebook

You may print this ebook for your personal use. Handing over printouts is not permitted.

Some process pictures are of greater size than A4 for readability purposes. Hence you have to activate poster printing on your printer when printing these process pictures. This will allow to print them distributed to more than one sheet.
# Content

1. Content............................................................................................................................. 4
2. The novelties within ITIL® V3 revision 2011................................................................. 6
3. Service Lifecycle............................................................................................................. 9
4. Service Operation............................................................................................................ 14
   4.1 Process Overview....................................................................................................... 14
   4.2 Interfaces.................................................................................................................. 15
   4.3 Processes within Service Operation......................................................................... 23
      4.3.1 Event Management............................................................................................ 25
         4.3.1.1 Interfaces................................................................................................. 26
         4.3.1.2 Organization of Event Management......................................................... 30
         4.3.1.3 Event Monitoring...................................................................................... 36
         4.3.1.4 Event Tracking and Closure...................................................................... 41
      4.3.2 Incident Management......................................................................................... 46
         4.3.2.1 Interfaces................................................................................................. 47
         4.3.2.2 Organization of Incident Management.................................................... 55
         4.3.2.3 Incident Registration................................................................................. 63
         4.3.2.4 Incident Resolution First Level................................................................. 70
         4.3.2.5 Incident Resolution Second Level............................................................ 78
         4.3.2.6 Incident Monitoring and Escalation......................................................... 85
         4.3.2.7 Major Incidents......................................................................................... 91
         4.3.2.8 Incident Tracking and Closure................................................................. 98
         4.3.2.9 User Information....................................................................................... 103
         4.3.2.10 Incident Reporting.................................................................................. 106
      4.3.3 Problem Management......................................................................................... 109
         4.3.3.1 Interfaces................................................................................................. 110
         4.3.3.2 Problem Registration............................................................................... 115
         4.3.3.3 Problem Resolution................................................................................. 120
         4.3.3.4 Problem Tracking and Closure............................................................... 127
         4.3.3.5 Review of Major Problems........................................................................ 132
         4.3.3.6 Problem Reporting.................................................................................... 136
      4.3.4 Access Management............................................................................................ 139
         4.3.4.1 Interfaces................................................................................................. 140
         4.3.4.2 Enlistment and Retirement...................................................................... 145
         4.3.4.3 Management of User Profiles................................................................. 156
         4.3.4.4 User Permission Request......................................................................... 162
      4.3.5 Service Request................................................................................................... 168
         4.3.5.1 Interfaces................................................................................................. 169
         4.3.5.2 Service Request....................................................................................... 173
         4.3.5.3 Backup Recovery....................................................................................... 178
### Checklists for Service Operation

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Checklist Request for Change</td>
<td>236</td>
</tr>
<tr>
<td>7.2 Checklist Incident Record</td>
<td>238</td>
</tr>
<tr>
<td>7.3 Checklist Initial Analysis of Incident</td>
<td>240</td>
</tr>
<tr>
<td>7.4 Checklist Incident Priority</td>
<td>242</td>
</tr>
<tr>
<td>7.5 Checklist Incident Escalation</td>
<td>244</td>
</tr>
<tr>
<td>7.6 Checklist Incident Management Report</td>
<td>245</td>
</tr>
<tr>
<td>7.7 Checklist Capacity Reporting</td>
<td>247</td>
</tr>
<tr>
<td>7.8 Checklist Operational Level Agreement</td>
<td>249</td>
</tr>
<tr>
<td>7.9 Checklist Continual Service Improvement Register</td>
<td>253</td>
</tr>
<tr>
<td>7.10 Checklist Service Level Requirement</td>
<td>255</td>
</tr>
<tr>
<td>7.11 Checklist Service Level Agreement</td>
<td>256</td>
</tr>
<tr>
<td>7.12 Checklist Service Level Report</td>
<td>260</td>
</tr>
<tr>
<td>7.13 Checklist Service Catalogue</td>
<td>262</td>
</tr>
<tr>
<td>7.14 Checklist Service Portfolio</td>
<td>263</td>
</tr>
<tr>
<td>7.15 Checklist Service Design Package</td>
<td>266</td>
</tr>
<tr>
<td>7.16 Checklist Service Specification</td>
<td>270</td>
</tr>
<tr>
<td>7.17 Checklist Availability Reporting</td>
<td>274</td>
</tr>
<tr>
<td>7.18 Checklist Underpinning Contract</td>
<td>276</td>
</tr>
<tr>
<td>7.19 Checklist Problem Record</td>
<td>279</td>
</tr>
<tr>
<td>7.20 Checklist Problem Priority</td>
<td>281</td>
</tr>
<tr>
<td>7.21 Checklist Problem Closing</td>
<td>283</td>
</tr>
</tbody>
</table>
2 The novelties within ITIL® V3 revision 2011

Since the publication of the ITIL® V3 more than 500 improvement proposals (changes and completion) for the roles, processes and interfaces have been provided from the users and the training organizations as well. This has been major input for the description of the IT Service life cycle. Requirements from the Sarbanes - Oxley Act (SOX) have been added thus providing improved transparency of the processes. Outsourcing and cloud strategies have been requiring enhanced security management with tightened control and documentation duties.

Roles, interfaces, inputs and outputs have been harmonized within the five publications, errors and inconsistencies in text and graphics have been removed. Hence the edition 2011 is more easy to read, control, translate, implement and communicate.

The ITIL® 2011 edition is available in English printing since the end of july 2011. A German translation is available since april 2013.

The changes in detail

Service Strategy

Main issue of the update was an increased comprehensibility of this ITIL® discipline.

New processes have been added:

- Strategy Management for IT Services (Development and maintenance of the IT Service Strategy, harmonization with the business strategy)
- Business Relationship Management
- Demand Management

The process Financial Management has been enhanced.

Service Design

Main issue is the clarification of the integration into Service Strategy to ensure the strategic and customer oriented requirements. This is represented within the processes and management activities in the Service Design by the new process of Design Coordination. Another important improvement of the comprehensibility regards the 5 aspects of service quality

- Design of tools for service management
- Service Portfolio and Service Catalogue
- Architecture for services and tools of service management
- Processes
- Measurements (performance indicators and methods of measurement).
Service Transition

The structure, content and relations of the Configuration Management System (CMS) and the Service Knowledge Management System (SKMS) have been described in more detail. New is the Change Proposal and its usage. The scope of the evaluation process, now renamed to Change Evaluation, has been enhanced. The asset management is now enhanced within Service Asset and Configuration Management. The processes

- Change Management
- Change Evaluation
- Release and Deployment Management

are integrated in more detail.

Service Operation

Most of the processes have been actualized and complemented, especially

- Event Management (especially rules and methods for automated caption and analysis)
- Problem Management (especially proactive Problem Management)
- Access Management
- Request Fulfillment (request models).

Application Management has been distinguished better from Application Development and the correlation has been explained. Further clarifications have been introduced with the techniques of problem analysis, procedures for Incident Matching and escalation of incidents to Problem Management. Furthermore, the description of the management of physical infrastructure (Facility Management) has been broadened.

Continual Service Improvement

A special focus was given to the documentation of the interfaces of Continual Service Improvement to the other life cycle phases. The 7 step improvement process

- what has to be measured
- what can be measured
- measurement process
- preparation of data
- analysis of data
- presentation
- deduction of corrective actions

and its relation to the Deming Cycle and the Knowledge Management has been clarified. The CSI Model has been renamed to CSI Approach, the CSI Register as container for all details of all improvement initiatives within the organization has been introduced.
The impacts

All previous ITIL® V3 certifications remain valid as the introduced modifications have no greater impact to the basic concepts of the service life cycle.

Based upon the edition 2011 minor adjustments to the training contents and certification tests have been introduced.
4 Service Operation

The discipline Service Operation is responsible for the economic and friction free productive operation of the IT Services including handling of emergency situations. This comprises especially the efficient management of Events (extraordinary system conditions), Incidents (failures) and Problems (causes for repetitive failures). Furthermore it takes responsibility for the control of User Profiles and User Permissions, and the related access rights for IT Services, IT Systems and data.

4.1 Process Overview
4.2 Interfaces
Process Details

Process Responsible: IT Manager
Process Content: First level processes for efficient and effective IT Service Operation.
ISO20000 relevant: yes
ISO9000ff relevant: yes
SOX relevant: yes

Involved Organizational Units and Roles

IT Service Consumers
Suppliers
ITSM Disciplines outside Service Operation
Service Operation

Subprocesses

Business Processes (Task)
Operational processes of the organization of the IT Service Consumers.

Business Unit: IT Service Consumers

Data Objects
- User Information (incoming)
- Emergency Procedure (incoming)
- Backup Recovery Request (outgoing)
- Retirement Notification (outgoing)
- Request for User Account (outgoing)
- Request for User Permission (outgoing)
- Enlistment Notification (outgoing)
- Organizational Change (outgoing)
- Service Request (outgoing)
- Incident Message (outgoing)

Human Resource Processes (Task)
Human resource processes of the organization of the IT Service Consumers.

Business Unit: IT Service Consumers
Data Objects

- Retirement Notification (outgoing)
- Enlistment Notification (outgoing)

Supplier Process (Task)
Processes of the external Suppliers of the responsible IT Service Provider.

Business Unit
Suppliers

Data Objects
- Request 3rd Level Support (incoming)

Service Strategy (Collapsed Subprocess)
Company wide definition and periodic further development of the company strategy of the organization of the IT Service Strategy as part of the company strategy and IT Financial Management as well.

Business Unit
ITSM Disciplines outside Service Operation

Data Objects
- Complaint (incoming)
- Incident Management Report (incoming)
- Problem Management Report (incoming)

Service Design (Collapsed Subprocess)
Processes for the design and development respective modifications and enhancements of the IT Services.

Business Unit
ITSM Disciplines outside Service Operation

Data Objects
- Equipment Requirement (incoming)
- License Requirement (incoming)
- Event Statistics (incoming)
- Incident Management Report (incoming)
- IT Requirements Request (incoming)
- Emergency Procedure (incoming)
- Problem Management Report (incoming)
- Security Relevant Occurrence (incoming)
- Request for Personnel Resources (outgoing)
- Availability Management Report (outgoing)
- User Equipment (outgoing)
- Capacity Management Report (outgoing)
- IT Requirements for Recovery (outgoing)
- IT Service Continuity Report (outgoing)
- Licenses (outgoing)
- Emergency (outgoing)
- Problem Susicion (outgoing)
- Risk Message (outgoing)
- Risk Log (outgoing)
- Security Management Report (outgoing)
- Service Request (outgoing)
- Security Alert (outgoing)

**Service Transition (Collapsed Subprocess)**
Processes for the controlled transfer of the IT Services respective modifications to IT Services to Service Operation.

*Business Unit*
ITSM Disciplines outside Service Operation

*Data Objects*
- Order for Problem Solution (incoming)
- User Role (incoming)
- Change Record (incoming)
- Emergency Request for Change (incoming)
- Equipment Status (incoming)
- Event Statistics (incoming)
- Incident Management Report (incoming)
- License Status (incoming)
- Emergency Procedure (incoming)
- Problem Management Report (incoming)
- Request for Change (incoming)
- Request for Personnel Resources (outgoing)
- Change Record (outgoing)
- Change Schedule (outgoing)
- Planned Service Outage (outgoing)
- New / modified IT Service (outgoing)
- Release Record (outgoing)
- Service Request (outgoing)
- Transition Management Report (outgoing)

**Continual Service Improvement (Collapsed Subprocess)**
Processes for continual quality assurance and improvement of the IT Services.

*Business Unit*
ITSM Disciplines outside Service Operation
Data Objects

- Incident Management Report (incoming)
- Problem Management Report (incoming)
- Recommendation for Process Quality Improvement (incoming)
- Recommendation for Service Quality Improvement (incoming)

Event Management (Collapsed Subprocess)
Automated and manual surveillance of IT Systems and IT Services, and introduction of necessary activities thereof.

Business Unit
Service Operation

Data Objects

- Availability Management Report (incoming)
- Capacity Management Report (incoming)
- IT Service Continuity Report (incoming)
- Risk Log (incoming)
- Event Incident Notice (outgoing)
- Event Statistics (outgoing)
- Event Ticket (outgoing)

Incident Management (Collapsed Subprocess)
Handling of Incidents over their life cycle.

Business Unit
Service Operation

Data Objects

- Backup Recovery Request (incoming)
- Retirement Notification (incoming)
- User Account set up (incoming)
- User Account deleted (incoming)
- Request for User Account (incoming)
- User Role (incoming)
- Request for User Permission (incoming)
- Complaint (incoming)
- Enlistment Notification (incoming)
- Event Incident Notice (incoming)
- Event Statistics (incoming)
- Event Ticket (incoming)
- Planned Service Outage (incoming)
- IT Operations Schedule (incoming)
- Known Error (incoming)
Problem Management Report (incoming)
Problem Record (incoming)
Resource Planning (incoming)
Risk Message (incoming)
Backup Recovery performed (incoming)
Security Management Report (incoming)
Service Request (incoming)
Security Alert (incoming)
Standard Operating Procedures (incoming)
Status Service Request (incoming)
Transition Management Report (incoming)
Workaround (incoming)
Request 3rd Level Support (outgoing)
Backup Recovery Request (outgoing)
User Information (outgoing)
Complaint (outgoing)
Incident Management Report (outgoing)
Emergency (outgoing)
Problem Record (outgoing)
Problem Suspicion (outgoing)
Service Request (outgoing)
Security Relevant Occurrence (outgoing)

Problem Management (Collapsed Subprocess)
Handling of Problems over their life cycle.

Business Unit
Service Operation

Data Objects
Change Schedule (incoming)
Event Statistics (incoming)
Incident Management Report (incoming)
Problem Record (incoming)
Problem Suspicion (incoming)
Resource Planning (incoming)
Order for Problem Solution (outgoing)
Known Error (outgoing)
Problem Management Report (outgoing)
Problem Record (outgoing)
Request for Change (outgoing)
Recommendation for Process Quality Improvement (outgoing)
Service Operation according to ITIL® 2011

- Recommendation for Service Quality Improvement (outgoing)
- Workaround (outgoing)

Access Management (Collapsed Subprocess)
Grant of business conforming access of the users to IT Services and avoiding of unauthorized access.

Business Unit
Service Operation

Data Objects
- User Equipment (incoming)
- Licenses (incoming)
- New / modified IT Service (incoming)
- Organizational Change (incoming)
- Request for User Account (incoming)
- Equipment Requirement (outgoing)
- License Requirement (outgoing)
- User Account set up (outgoing)
- User Account deleted (outgoing)
- User Role (outgoing)
- Equipment Status (outgoing)
- License Status (outgoing)

Service Request (Collapsed Subprocess)
Handling of Service Requests.

Business Unit
Service Operation

Data Objects
- Backup Recovery Request (incoming)
- Request for Data Recovery (incoming)
- Service Request (incoming)
- Backup Recovery performed (outgoing)
- Status Service Request (outgoing)
- Request for User Account (outgoing)
- Data restored (outgoing)

Operations Control (Collapsed Subprocess)
Control and monitoring of the IT Services and the IT Infrastructure.

Business Unit
Service Operation
Data Objects

- Request for Personnel Resources (incoming)
- Availability Management Report (incoming)
- Capacity Management Report (incoming)
- Change Record (incoming)
- Event Statistics (incoming)
- Incident Management Report (incoming)
- IT Requirements for Recovery (incoming)
- IT Service Continuity Report (incoming)
- Emergency (incoming)
- Problem Management Report (incoming)
- Release Record (incoming)
- Risk Log (incoming)
- Data restored (incoming)
- Request for Data Recovery (outgoing)
- Change Record (outgoing)
- Emergency Request for Change (outgoing)
- IT Requirements Request (outgoing)
- IT Operations Schedule (outgoing)
- Emergency Procedure (outgoing)
- Problem Suspicion (outgoing)
- Resource Planning (outgoing)
- Standard Operating Procedures (outgoing)
4.3 Processes within Service Operation

The IT Service Management processes of Service Operation contain the following:

- **Event Management**
  - Event Management - Interfaces
  - Organization of Event Management
  - Event Monitoring
  - Event Tracking and Closure

- **Incident Management**
  - Incident Management - Interfaces
  - Organization of Incident Management
  - Incident Registration
  - Incident Resolution First Level
  - Incident Resolution Second Level
  - Incident Monitoring and Escalation
  - Major Incidents
  - Incident Tracking and Closure
  - User Information
  - Incident Reporting

- **Problem Management**
  - Problem Management - Interfaces
  - Problem Registration
  - Problem Resolution
  - Problem Tracking and Closure
  - Review of Major Problems
  - Problem Reporting

- **Access Management**
  - Access Management - Interfaces
  - Enlistment and Retirement
  - Management of User Profiles
  - User Permission Request
- Service Request
  - Service Request - Interfaces
  - Service Request
  - Backup Recovery

- Operations Control
  - Operations Control - Interfaces
  - IT Operations Management
  - Contingency Activities
4.3.2 Incident Management

Incident Management is responsible for the efficient resolution of all kinds of Incidents and fastest possible return to standard operation after such Incidents.

This contains basically the following subprocesses:

- Organization of Incident Management
- Incident Registration
- Incident Resolution First Level
- Incident Resolution Second Level
- Incident Monitoring and Escalation
- Major Incidents
- Incident Tracking and Closure
- User Information
- Incident Reporting.

This process group was already part of the previous version of ITIL®.

In the following paragraphs the subprocesses of this process group are described in detail.
4.3.2.4 Incident Resolution First Level
Process Details

Process Responsible: Incident Manager
Process Content: Immediate Resolution of the Incident as far as possible in agreed schedule, otherwise transfer to 2nd Level Support.
Process Goal: Fastest possible solution for Incidents within the agreed time frames and earliest possible handover to 2nd Level Support in case of no immediate solution possible.
ISO20000 relevant: yes
ISO9000ff relevant: yes
SOX relevant: yes

Involved Organizational Units and Roles

1st Level Support
Initiator of Incident
Information Security Manager
IT Operations

Process Flow

Incident recorded (Start Signal Event)

Business Unit
1st Level Support

Initial analysis of Incident (Task)
The Incident is initially analyzed according to the criteria
- Major Incident
- Security Relevant Occurrence
- Complaint.
Complaints are prequalified prior to handover to Feedback Management.

Business Unit
1st Level Support

Accompanying Documents
- Checklist Initial Analysis Incident (Document)
### Incident / Major Incident / Security Relevant Occurrence / Qualified Complaint (Data Based Exclusive Gateway)

**Business Unit**  
1st Level Support

<table>
<thead>
<tr>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Security Relevant Occurrence&quot;</td>
<td>Forward ticket to Security Management (Task)</td>
</tr>
<tr>
<td>&quot;Major Incident&quot;</td>
<td>Forward ticket to Major Incident Team (Task)</td>
</tr>
<tr>
<td>&quot;Qualified Complaint&quot;</td>
<td>Forward complaint to Feedback Management (Task)</td>
</tr>
<tr>
<td>&quot;Incident&quot;</td>
<td>Search for relevant documented solution hints (Task)</td>
</tr>
</tbody>
</table>

**Forward ticket to Major Incident Team (Task)**

The Incident Ticket is forwarded to the Major Incident Team.

**Ticket forwarded to Major Incident Team (End Signal Event)**

**Business Unit**  
1st Level Support

**Glossary Item**  
Major Incident Team (Organisation)

**Forward complaint to Feedback Management (Task)**

The qualified complaint is forwarded to Feedback Management.

**Qualified complaint forwarded to Feedback Management (End Signal Event)**

**Business Unit**  
1st Level Support

**Search for relevant documented solution hints (Task)**

For resolution based upon the initial analysis the knowledge base of Incident Management is searched for relevant comparable Incidents and their resolutions.

**Business Unit**  
1st Level Support

**Data Repositories**  
Service Desk System
Determine whether directly solvable *(Task)*
The decision about the immediate solvability by 1st Level Support is made.

*Business Unit*
1st Level Support

**Solvable by 1st Level Support? (Data Based Exclusive Gateway)**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>„no“</td>
<td>Define responsible in 2nd Level Support <em>(Task)</em></td>
</tr>
<tr>
<td>„yes“</td>
<td><strong>Workaround</strong> required? <em>(Data Based Exclusive Gateway)</em></td>
</tr>
</tbody>
</table>

**Workaround required? (Data Based Exclusive Gateway)**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>„no“</td>
<td>Resolve Incident causally <em>(Task)</em></td>
</tr>
<tr>
<td>„yes“</td>
<td>Implement <strong>Workaround</strong> <em>(Task)</em></td>
</tr>
</tbody>
</table>

**Resolve Incident causally (Task)**
The Incident is resolved causally.

*Business Unit*
1st Level Support

**Check completeness and effectivity (Task)**
The completeness and effectivity of the workaround for Incident resolution is verified.

*Business Unit*
1st Level Support

**Actualize Configuration Items (Task)**
As far as the Incident resolution changed Configuration Items they are actualized.

*Business Unit*
1st Level Support

*Data Repositories*
Configuration Management System

**Verify immediate effectivity with Initiator (Task)**
The immediate effectivity of the Incident resolution is verified with the Initiator.

*Business Unit*
1st Level Support
Additional Participants

- Initiator of Incident

Effective? *(Data Based Exclusive Gateway)*

<table>
<thead>
<tr>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>„no“</td>
<td>Check the available time for resolution (Task)</td>
</tr>
<tr>
<td>„yes“</td>
<td>Document Incident resolution (Task)</td>
</tr>
</tbody>
</table>

**Implement workaround** *(Task)*

In case the immediate resolution needs a **Workaround** it is implemented.

**Business Unit**

1st Level Support

**Check completeness and effectivity** *(Task)*

The completeness and effectivity of the **Workaround** for Incident resolution is verified.

**Business Unit**

1st Level Support

**Actualize Configuration Items** *(Task)*

As far as the implementation of the **Workaround** changed **Configuration Items** they are actualized.

**Business Unit**

1st Level Support

**Data Repositories**

**Configuration Management System**

**Verify immediate effectivity with Initiator** *(Task)*

The immediate effectivity of the **Workaround** is verified with the Initiator.

**Business Unit**

1st Level Support

**Additional Participants**

- Initiator of Incident

**Capture Problem Record to Incident** *(Task)*

For the Incident resolved by **Workaround** (means not causally resolved) a **Problem Record** is captured which triggers the processing by Problem Management.

**Business Unit**

1st Level Support
Effective ? *(Data Based Exclusive Gateway)*

*Business Unit*  
1st Level Support

<table>
<thead>
<tr>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;no&quot;</td>
<td>Check the available time for resolution (Task)</td>
</tr>
<tr>
<td>&quot;yes&quot;</td>
<td>Document Incident resolution (Task)</td>
</tr>
</tbody>
</table>

**Document Incident resolution (Task)**

The resolution of the Incident is documented in the knowledge base of Incident and Problem Management.

*Business Unit*  
1st Level Support

*Data Repositories*  
Service Desk System

**Set Incident Status to "resolved" (Task)**

The status of the Incidents is set to "resolved".

*Business Unit*  
1st Level Support

*Data Repositories*  
Service Desk System

**Inform Initiator (Collapsed Subprocess)**

The Initiator of the Incident is informed about the resolution.

*Business Unit*  
1st Level Support

**Incident resolved (End Signal Event)**

*Business Unit*  
1st Level Support

**Check the available time for resolution (Task)**

In case the resolution by *Workaround* was not effective the residual resolution time is checked to determine a decision about handover to *2nd Level Support*.
Agreed resolution time in danger? *(Data Based Exclusive Gateway)*

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>Condition</th>
<th>Subsequent Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td>„no“</td>
<td>Determine whether directly solvable (Task)</td>
</tr>
<tr>
<td>1st Level Support</td>
<td>„yes“</td>
<td>Define responsible in 2nd Level Support (Task)</td>
</tr>
</tbody>
</table>

Incident reported to Problem Management *(End Signal Event)*

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>1st Level Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td></td>
</tr>
</tbody>
</table>

Define responsible in 2nd Level Support *(Task)*

In case the Incident is not directly solvable by 1st Level Support the competent person or group in 2nd Level Support is identified.

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>1st Level Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td></td>
</tr>
</tbody>
</table>

Data Repositories

<table>
<thead>
<tr>
<th>Service Desk System</th>
</tr>
</thead>
</table>

Forward ticket to 2nd Level Support *(Task)*

The Incident Ticket is forwarded to 2nd Level Support.

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>1st Level Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td></td>
</tr>
</tbody>
</table>

Data Repositories

<table>
<thead>
<tr>
<th>Service Desk System</th>
</tr>
</thead>
</table>

Ticket forwarded to 2nd Level Support *(End Signal Event)*

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>1st Level Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td></td>
</tr>
</tbody>
</table>

Glossary Item

<table>
<thead>
<tr>
<th>2nd Level Support (Organisation)</th>
</tr>
</thead>
</table>

Forward ticket to Security Management *(Task)*

The Incident Ticket is forwarded to Security Management.

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>1st Level Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level Support</td>
<td></td>
</tr>
</tbody>
</table>
Inform Security Management *(Task)*

Security Management is informed instantaneous about the security relevant Incident.

*Business Unit*

1st Level Support

*Additional Participants*

- Information Security Manager

Security Relevant Occurrence forwarded to Security Management *(End Signal Event)*

*Business Unit*

1st Level Support

Involved IT Systems

- Service Desk System
- Configuration Management System
5 Glossary

5.1 Process Documents in Service Operation

Availability Management Report
The Availability Management Report informs the other ITSM functions about the availability of IT Services and IT Infrastructure.
Applicable Documents
Checklist Availability Reporting

Capacity Management Report
The Capacity Management Report contains all relevant information about usage and performance of the IT Services and IT Infrastructure.
Applicable Documents
Checklist Capacity Reporting

Change Model
Change Models define the content and the procedure for Standard Changes. These are pre-approved Changes with low risk.

Change Record
The Change Record is based upon the Request for Change and documents the complete life cycle of a Change.

Change Schedule
The Change Schedule (Forward Schedule of Changes) contains the planning of all approved Changes including their accompanying information and dependencies.

Configuration Item
Configuration Items are the operating resources of the IT services in general. They are maintained within the Configuration Management Database (CMDB), which itself is a core component of the Configuration Management System.

Continual Service Improvement Register
The Continual Service Improvement Register (CSI Register) is the basis for all potentials and initiatives for the improvement of the service quality over the service life cycle. In the cyclic CSI Register all activities to improve the service quality are documented.
Applicable Documents
Checklist CSI Register
Emergency
An Emergency is a complex breakdown of IT Systems and/or IT Services, e.g.:
- complete breakdown of one or more IT Systems
- blackout of a subsidiary caused by damage or ruin of IT Infrastructure
- disaster situations

Emergency Procedure
Emergency Procedures define all activities for the fastest possible restore of operation of IT Systems after emergency situations (disasters, complete breakdown of IT Services or locations, aso.). This restore has normally two steps:
- recovery of a life-sustaining minimal operation
- recovery of full operation.

Event Correlation
The Event Correlation describes the relations between events and necessary operational interventions respective necessary error messages. The rules for the Event Correlation define the appropriate reaction to an Event.

Event Incident Notice
Message about a recognized malfunction of an IT System or an IT System Component from Event Management.

Event Record
The Event Record describes relevant status changes from the operation of IT Services and IT Infrastructure Components. They may be status changes but also alarm situations.

Event Statistics
The Event Statistics shows patterns and trends of Events and allows an analysis of the efficiency of the Event Recognition.

Event Ticket
Automated message about a recognized malfunction of an IT System or an IT System Component from the Event Management to the Service Desk System.

Improvement Management Report
The Improvement Report provides information about planning and results of Continual Service Improvement for the other IT Service Management functions. It contains planned, actually executed and since the last report finished service- and process improvement activities and their expected respective achieved results. Furthermore proposals for future additional service improvement activities are provided.
Incident Escalation Rules
The Escalation Rules for Incidents define the hierarchy levels for escalation of an Incident and the triggers therefore.

Applicable Documents
Checklist Incident Escalation Rules

Incident Management Report
The Incident Management Report informs all involved ITSM Disciplines about occurred Incidents and their elimination.

Applicable Documents
Checklist Incident Management Report

Incident Message
Message by an IT Service Consumer or an IT employee about a recognized malfunction of an IT System or an IT System Component.

Incident Model
Incident Models describe the predefined activities to handle known and recurring types of Incidents and their effective and efficient elimination.

Incident Record
The Incident Record contains all information about an Incidents over its lifecycle. Typically it is documented in the Service Desk System.

Applicable Documents
Checklist Incident Record

IT Budget
The IT Budget is a rolling business period related financial plan containing a prognosis of expenses and revenues to be expected for the IT Organization. Within the IT Budget funds are allocated to the processes of the IT Service Management respective to the organizational units of the IT Service Provider.

IT Operations Schedule
The IT Operations Schedule contains the planning of all recurring activities for the maintenance of operation for the IT Systems and a friction free IT Operation:

• system specific planning of backups
• reorganisation of IT Systems
• system maintenance
• data cleansing
• data archiving
• batch jobs
• aso.
IT Requirements Request
An IT Requirements Request represents an application for procurement of services and/or goods from external Suppliers of the IT. The IT Requirements Request describes the contents of the demand and is transformed into a definitive purchasing requisition within the IT Procurement Process.

IT Service Continuity Report
The IT Service Continuity Report informs about the actual status of Contingency Planning and the actual Emergency Procedures.

Known Error
A Known Error is a Problem whose cause is known and documented including a documented Workaround (as far as available).

Major Incident
A Major Incident is an Incident with serious negative impact on the business activities of the company.

Operational Level Agreement
The Operational Level Agreement provides an internal contract between the IT Service Provider and another part of the IT Organization regarding the provision of an IT Service Contribution. It defines besides others:

- a description of the Service Contribution
- the Service Level goals
- the mutual responsibilities.

Applicable Documents
Checklist Operational Level Agreement

Operational Task
Operational Tasks are routine tasks to maintain friction free operation of IT services:

- backup
- data cleansing
- reorganization of IT systems
- archiving
- necessary batch processes
- print services
- aso.

Planned Service Outage
Planned Service Outages due to the implementation of Changes by Service Transition. These Planned Service Outages are normally within the maintenance time frames according to the Service Level Agreements and thus do not reduce the contractual agreed Availability of the respective IT Services.
Problem Management Report
The Problem Management Report informs all involved ITSM Disciplines about open Problems and Problems in process and the related solutions and Workarounds.

Problem Record
The Problem Record contains all information of a Problem over its lifecycle. Typically it is documented in the Service Desk System.

Applicable Documents
Checklist Problem Record

Purchase Order
The Purchase Order is the binding order to the Supplier to deliver the goods and/or services specified in the purchase order under the conditions described there respective in accompanying related documents.

Recommendation for Process Quality Improvement
Trigger for the optimization of the quality of IT processes as input for the process review.

Recommendation for Service Quality Improvement
Trigger for the optimization of the quality of IT services and IT infrastructure services by changes in:
- Service Level Agreements
- Operational Level Agreements
- Underpinning Contracts

as input for the Service Review.

Release Package
The release package contains all Configuration Items belonging to the respective release. Those Configuration Items may be:
- hard- and software components
- IT infrastructure services
- IT applications
- aso.

Release Record
The Release Record documents the complete lifecycle of a Transition Project.

Request 3rd Level Support
Notification of a detected malfunction of an IT System respective IT System Component within a externally provided IT Service respective IT Service Contribution to the external Supplier.
Request for Change
The Request for Change is a formal request to perform a Change required for all types of Change not defined as release free Standard Change.

Applicable Documents
Checklist Request for Change

Request for User Account
The Request for User Account is an application for installation of an user access within an IT System. This installation requires an authorization by a respective User Role and the availability of licenses for the involved IT system as well.

Request for UserPermission
The Request for User Permission is an application for installation, modification or deletion of User Permissions within an IT system.

Risk Log
The Risk Log is a rated catalogue of identified risks and accordingly defined activities for minimization and mitigation.

Risk Message
Message about recognized necessary activities from Risk Management.

Security Alert
A Security Alert serves as initial information about newly recognized or even actually occurred security threats, providing the possibility to avoid or defend the threat for the receiver.

Security Management Report
The Security Management Report provides information about security relevant occurrences and activities and about the security situation of the IT Organization.

Service Catalogue
The Service Catalogue is the part of the Service Portfolio visible for the IT Service Consumers. It contains a complete listing of all active IT Services of the IT Service Provider including those released for deployment.

Applicable Documents
Checklist Service Catalogue

Service Contribution
A Service Contribution is a necessary part of the provision of an IT Service (Business Service), normally IT Basic or Infrastructure Services necessary to fulfill the Service Level Arrangements of the IT Services part of which they are.
Service Design Package
The Service Design Package describes the requirements to the development of IT Services based upon Service Level Requirements. It contains the requirements from the customer's perspective and describes how they will be realized from technical and organizational perspective.

Applicable Documents
Checklist Service Design Package

Service Documentation
The Service Documentation contains the complete description of the IT Services including all documentation needed for operation, maintenance and further development. This includes besides others:
- development documentation
- user documentation
- functional descriptions
- maintenance plans
- maintenance processes.

Service Landscape
The Service Landscape documents the relations between Business Services and IT Services at one hand and the relations between IT Services and IT Infrastructure at the other hand. Thus it assures the logical link from Business Service down to Configuration Items.

Furthermore it is the basis of a holistic Risk Management for the IT Services with the aspects:
- criticality from business perspective
- criticality from technology perspective
- criticality from resource perspective.

Service Level Agreement
The Service Level Agreement defines the mutual contractual requirements regarding the IT Service. This contains besides others:
- service description
- entitled Service Consumers
- Service Level Goals
- mutual responsibilities.

Applicable Documents
Checklist Service Level Agreement

Service Level Arrangement
Service Level Arrangements cover all service level relevant agreements and contracts:
- Service Level Agreements
- Operational Level Agreements
- Underpinning Contracts.
Service Level Report

The Service Level Report informs about the agreed service quality of the Service Providers respective Suppliers comparing the agreed and achieved Service Levels. The report furthermore provides information about the utilization of the IT Services, ongoing activities for Service Improvement and extraordinary occurrences.

Applicable Documents

Checklist Service Level Report

Service Level Requirement

The Service Level Requirement contains all requirements to an IT Service from the business perspective of the IT Service Consumers. It defines besides others:

- service requirements
- Service Level goals
- mutual responsibilities.

During service designs the Service Level Requirement is the basis for the service contract and the Service Level Agreement.

Applicable Documents

Checklist Service Level Requirement

Service Portfolio

The Service Portfolio contains a complete listing of all IT Services of the IT Service Provider:

- actual IT Services (contractual requirements defined by Service Level Agreements)
- new IT Services under development
- disabled IT Services.

Visible for the IT Service Consumers is the service catalogue (see there) as subset of the service portfolio.

Not visible for the IT Service Consumers are:

- IT Service Contributions defined by operational level agreements
- IT Service Contributions defined by Underpinning Contracts (external supplies defined by supplier contracts).

Applicable Documents

Checklist Service Portfolio

Service Request

Request from an IT Service Consumer or from an IT employee for:

- standard change
- user rights
- data recovery
- information
- consulting.
Service Strategy

Systematic, cyclic and operationalized long range planning of the goals of the IT Service Provider and for the IT services.

Standard Change

A Standard Change is a low risk recurring change, which does not need a explicit release by the Change Manager being generally released. Each standard change is described in a Change Model.

Standard Operating Procedures

The Standard Operating Procedures contain the rules for recurring standard activities of the IT Operation and the according targets for these activities and processes.

Transition Management Report

The Transition Management Report contains information about all active and planned Transition Projects (status, milestones, finish).

Underpinning Contract

An Underpinning Contract is a contract between the IT Service Provider and an external service supplier about the delivery of IT Service Contributions. It defines besides others:

- the description of the Service Contribution
- the service level goals
- the mutual responsibilities.

Applicable Documents

Checklist Underpinning Contract

User Information

Proactive information of the IT Service Consumers about

- the status of his/her Incident Message
- his/her Service Request
- occurrences influencing the availability of the consumed IT Services
- other miscellaneous information needs.

User Permission

The User Permission grants a defined scope of access to defined IT services or IT systems.

User Record

The User Record contains the system specific permissions of an User besides the identifying basic data.

User Role

The User Role describes the correlation of business oriented roles of users and the corresponding defined User Permissions in IT Systems.
Workaround

A Workaround is a bypass solution for an incident or a problem, where no cause eliminating solution is available so far. Goal of the workaround is to reduce or avoid the effects of the incident respective problem until a final solution is available.

Workarounds for incidents without related Problem Record are documented in their Incident Record, while workarounds for problems are documented in the Known Errors database.
5.2 Involved Organizational Units in Service Operation

**Controlling**

The organizational unit in charge for cost accounting, calculation, budgeting, cost control and monetary decision support (internal reporting).

**IT**

The responsible Service Provider.

**IT Applications**

The organizational unit or group inside the IT who is in charge for development, maintenance and support for IT applications.

**IT Operations**

The organizational unit or group inside the IT who is in charge for the IT Operation (infrastructure, operational services).

**IT Facilities**

IT Facilities are all assets plus organizational and technical environment to house the IT Infrastructure:

- computer rooms
- network distribution racks
- cooling and ventilation
- power supply
- access control infrastructure
- monitoring systems for the IT Infrastructure
- aso.
### Involved Roles in Service Operation

#### 1st Level Support
The responsibility of 1st Level Support is to register and classify incoming notifications. In case of incident messages, he/she undertakes an immediate effort to restore a failed IT service as quickly as possible in case of foreseeable success. If no ad hoc solution can be achieved, 1st Level Support will transfer the incident to the appropriate technical support groups (2nd Level Support). 1st Level Support also processes Service Requests of Users and keeps Users informed about their notifications’ status at agreed intervals or status changes.

#### 2nd Level Support
2nd Level Support takes over incidents which cannot be solved immediately by the means of 1st Level Support. If necessary, he/she will request external support, e.g. from software or hardware manufacturers (3rd Level Support). The goal is to restore a failed IT Service as quickly as possible, if necessary by implementation of a Workaround. If no causal solution can be found, the 2nd Level Support passes on the incident to Problem Management for further processing.

#### 3rd Level Support
3rd Level Support is typically located at external Suppliers (hardware or software manufacturers). Its services are requested by 2nd Level Support if their technical expertise is not sufficient respective additional skills are required for solving an incident or problem. The goal is to restore a failed IT Service as quickly as possible.

#### Access Manager
The Access Manager is responsible for approvals of permissions to use an IT Service, data and other IT Assets for authorized Users based upon the specifications of the IT Security Management and cares for the prevention of access for unauthorized Users at the same time.

#### Application Manager
The Application Manager is responsible for operation of, the User support resources in 2nd Level Support for and the support of further development of the applications in his area over their life cycle.

#### Availability Manager
The Availability Manager is responsible for the definition, analysis, planning, measuring and improvement of all aspects of the availability of IT Services in respect to the agreed service levels. He/she is responsible for ensuring that all IT Infrastructure, processes, tools, roles and other utilized auxiliary means are appropriate for the agreed service level targets of availability (also in the future based upon known business requirements).

#### Capacity Manager
The Capacity Manager is responsible for ensuring that IT Services and IT Infrastructure are able to deliver the agreed service levels from capacity perspective in a cost effective manner. He/she is responsible for ensuring that all IT infrastructure, processes, tools, roles and other utilized auxiliary means are appropriate for the agreed service level targets of capacity (also in the future based upon known business requirements).
Change Advisory Board
The Change Advisory Board is a team from all organizational units of the IT Service Provider, its customers and (as far as necessary) Suppliers, advising the Change Management in classifying, evaluating, prioritizing, scheduling and releasing of changes. It meets on a periodical basis.

Change Manager
The Change Manager authorises, documents and controls all changes in the IT services, the IT infrastructure and their components (Configuration Items (CI)) over the change lifecycle, in order to maintain a minimum amount of interruptive effects upon the running operation. In the case of further reaching changes, he/she involves the Change Advisory Board (CAB), in emergency cases the Emergency Change Advisory Board (ECAB).

Compliance Manager
The Compliance Manager's responsibility is to ensure that standards and guidelines are followed. This covers
- proper and consistent accounting
- obeying of procurement guidelines
- obeying environmental regulations and law
- obeying other statutory provisions
- obeying other company specific regulations.

Continual Service Improvement Manager
The Continual Service Improvement Manager is responsible for managing improvements to the IT Services and the IT Service Management processes over their life cycle regarding the development of business requirements and the IT Service Strategy. He/she continually measures the performance of the IT Service Provider and designs improvements to IT Services, IT Infrastructure and IT Processes in order to increase efficiency, effectiveness, and profitability of the IT Service Provider.

Emergency Change Advisory Board
The Emergency Change Advisory Board is a team consisting of members of the Change Advisory Board, called by the Change Manager on short notice in Emergency cases, who make decisions about high impact emergency changes. Selection of members of the Emergency Change Advisory Board is decided at the time a meeting is called depending on the nature of the emergency change.

Financial Manager
The Financial Manager is responsible for managing the IT Service Provider's financials containing
- budgeting
- accounting and cost control
- charging of deliverables provided to the customer.

Incident Manager
The Incident Manager is primarily responsible for the fastest possible restoring of a failing IT System in case of incidents. He/she is the first stage of escalation for incidents in case they are not resolvable within the agreed service levels. Furthermore he/she is responsible for the intake and content conforming handover of customer messages of any kind (besides Incident Messages).
Information Security Manager
The Information Security Manager is responsible for ensuring the confidentiality, integrity and availability of an organization’s IT Services, IT Infrastructure, IT Assets, information and data (in all ways of presentation). He/she is usually involved in an organization wide approach to Security Management.

IT Controller
The IT Controller is the person in charge for the responsible Service Provider within the controlling department.

IT Facilities Manager
The IT Facilities Manager is responsible for the physical infrastructure housing the IT Infrastructure
- computer rooms
- power supply
- access controls
- cooling
- monitoring the environment.

IT Manager
Responsible manager of IT according to the organizational structure.

IT Operations Manager
The IT Operations Manager has the overall responsibility for all activities of IT operations:
- definition of the guidelines for routine tasks of IT operation (Standard Operating Procedures)
- ensuring that all operational routine tasks are performed in time and properly.

IT Operator
IT Operators are the staff who performs the ongoing operational activities:
- manual event monitoring
- performing backups
- ensuring that scheduled jobs are performed
- installation of standard equipment
- aso.

IT Service Consumer
All (internal and external) persons or organizational units, who consume the services of the IT Service Provider.
IT Service Continuity Manager

The IT Service Continuity Manager cares for the provision of the minimum service levels agreed upon in the Service Level Agreements in cases of disaster. To achieve this he/she

- arranges for risks that could seriously impact IT Services
- performs risk minimizing precautions for disaster situations by reducing the risk to an acceptable level
- plans activities for the recovery of IT Services in disaster cases.

ITSM Management

The group of leading persons inside the IT who are in charge for the disciplines of IT Service Management.

Major Incident Team

The Major Incident Team is an event driven arranged team of IT executives and technical experts lead by the Incident Managers concentrating on the resolution of a Major Incident (grave incident with influence on the company business).

Problem Manager

The Problem Manager is responsible that all problems are handled over their whole lifecycle to

- avoid the occurrence of incidents
- minimize the negative impacts of not avoidable incidents
- provide information about Known Errors
- document possible and implemented Workarounds
- detect possible future problems proactively.

Process Owner

The Process Owner is responsible for the friction free, economical and goal oriented operation of his/her process(es) (business process, IT process). This includes

- securing the necessary budgetary funding
- goal oriented economic design
- appropriate procedures of process controlling
- change management for the respective process
- continual process improvement.

Prospect

Possible future IT Service Consumers with defined demand for IT Services.

Release Manager

The Release Manager is responsible for planning, controlling and execution of rollouts from development to test to the live environments. His/her primary objective is to ensure that the integrity of the live environment is protected and that only beforehand tested components are released.
Risk Manager

The Risk Manager is responsible for identifying, assessing and controlling risks. This includes the
- analysis of criticality of IT Assets for the business
- analysis of possible threats for separate IT Assets
- evaluation of occurrence probability for different threats
- evaluation of occurrence effects for different threats
- definition of risk monitoring procedures
- definition of risk avoidance activities.

Service Catalogue Manager

The Service Catalogue Manager is responsible for developing and maintaining the service catalogue based upon the service portfolio, ensuring that all information within the service catalogue is accurate, up to date and accessible for all authorized persons.

Service Design Manager

The Service Design Manager is responsible that new respective existing services are designed that
- they are in accordance with the IT Service Strategy
- they can be provided in an economic way by the IT Service Provider
- all accompanying processes, guidelines and documentations for the operation of these services are existing
- all required responsibilities are defined and staffed with appropriately skilled personnel.

Service Level Manager

The Service Level Manager is responsible for the setting up executable Service Level Arrangements
- Service Level Agreements (customer oriented)
- Operational Level Agreements (operations oriented)
- Underpinning Contracts (supplier oriented)
in a way that the goals defined in these arrangements are reachable in economic manner. The achievement of goals is controlled and reported by him/her.

Service Owner

The Service Owner is responsible for the management of IT Service(s) assigned to him/her over their lifecycle. He/she supports the maintenance of the Service Strategy and the Service Portfolio.

Service Request Fulfillment Group

The Service Request Fulfillment Group specializes on the fulfilment of certain types of Service Requests. Typically, 1st Level Support will process simpler requests that can be answered immediately, while all others more extensive or more complex from content perspective are forwarded to the specialized fulfillment group in charge.
Supplier

External suppliers of IT Services, IT Service Contributions and outsourcing services, where the scope of supply is defined in the Underpinning Contracts, external suppliers of infrastructure and operating supplies.

Supplier Manager

The responsibility of the Supplier Manager covers

- the evaluation of qualified external Suppliers
- contract conclusions with external Suppliers meeting the business requirements
- lifecycle management of Underpinning Contracts
- ensuring correct fulfillment of contracts by the external Suppliers
- review and valuation of the external Suppliers’ performance.

User

The user of an IT System within the business organization (internal and external). Users are the purely operative subgroup of the IT Service Consumers.
5.4 Involved IT Systems in Service Operation

**Change Management Database**

The database of Change Management documenting all relevant information (Change Records) of all stages of the life cycle of Changes.

**Configuration Management System**

The Configuration Management System (CMS) contains a coherent logical model of the infrastructure of the IT organization. Within there is stored the information of all Configuration Items (CIs) maintained by the Configuration Management. This includes Configuration Records, Incident-, Problem- and Change - Information. The Configuration Management System may consist of a number of data bases connected via logical links.

**Event Database**

The Event Database contains all Event Records, acquired either automated from the Monitoring System or manually.

**Knowledge Management System**

The Knowledge Management System is the central repository of relevant knowledge information of the IT Service Providers. Ideally it is a structured document management system but may also consist of a mixture of IT supported and paper repository. In no case there should exist parallel archiving to the operational databases of the organisation but complement these seamlessly by following information categories:

- guidelines and procedures
- reports from all IT Service Management disciplines
- service- and project relevant information
- experience from project management
- process relevant information
- aso.

**Monitoring System**

The Monitoring System tracks the behaviour and the operation of IT Infrastructure Components and IT Infrastructure Services. It may be part of the monitored system or a separate surveillance system.

**Operational Systems**

The Operational Systems contain the whole of IT Systems of the enterprise which provide the functionality for the IT Services.

**Service Desk System**

The Service Desk System contains the database of user support including the knowledge base for Incident- and Problem Management. Normally it is part of the integrated IT Service Management system.
## 6.2 Responsibility Assignment Matrix for Incident Management

| Region | Activity | Change Control | Incident | Problem | Service Desk | Transfer | Transition | Incident Management | Service Operation | Service Strategy | Service Support | Service Delivery | Service Continuity | Service SLAs | Service Operations | Service Technology | Service Architecture |
|--------|----------|----------------|----------|---------|-------------|----------|------------|---------------------|------------------|-----------------|----------------|----------------|----------------|------------------|-------------|-------------------|----------------------|-------------------|

|       | Incident Management - Interface |        |          |         |             |          |            |                    |                  |                 |                |                 |                  |                 |                |
|-------|---------------------------------|--------|----------|---------|-------------|----------|------------|-------------------|------------------|-----------------|----------------|----------------|----------------|------------------|-------------|-------------------|----------------------|-------------------|

**Legend:**
- **A**: Responsible
- **B**: Authorised
- **C**: Consulted
- **D**: Informed
- **E**: Participates