CLAVIS klw AG
IT Service Management

Service Management

Infrastructure Management (including Monitors and Tools)

ICT IM designs, plans, deploys and operates the IT-infrastructure according to the plans and policies of IT Service Management (OLAS)

Incidents

Workarounds Resolutions

User

Requests Calls Information

uses

Customer (internal or external)

requires

concludes

agrees

pays for

SERVICES

substantiate

SLAs

measure

KPIs

proposes & agrees

Security Management

Security Management is responsible for the strategies and policies that IT Service Management and other processes have to implement

Security Incidents

Application Management

Application Development

Application Development is responsible for the planning, designing and building of new applications

Application Management is responsible for the overall management of the application as it goes through its entire lifecycle

External Providers

External Suppliers have an increasing importance for IT services as they deliver hardware, software and service. Underpinning contracts (UCs) with external providers define the agreements about the provision of certain elements of a service

Other Sources

implements

Service Desk

SURVEYS

Service Requests

Incidents
Service Requests

Workarounds
Resolutions

It is recommended that all members of the organisation be authorised to request Changes. Otherwise, innovation might be stifled or important concerns may go unreported. Even so, where there are large numbers of Users, it is suggested that User requests should require signature by a senior User manager prior to submission.

Changes

concludes

SLA breaches

Security Aspects

Facts on cost and prizing recommendations

Consolidated Input

Financial Plans
Budgets

Input to SLA

Agreed Targets for Availability, Reliability and Maintainability

Recommendations (SLA, Costing, Charging)

Recommendations (Costing, Charging)

RFCs

The SLM- process involves assessing the impact of Changes upon service quality and SLAs, both when Changes are proposed and after they have been implemented.

Request Fulfillment

Practice shows that handling of both failures in the infrastructure and of service requests are similar, and both are therefore included in the definition and scope of the process of Incident Management.
The word 'Incident' in this chapter applies to both, if not explicitly stated otherwise, although organisations may decide to develop their own service-request procedures to isolate them from the more technical issues.
if a service request has been made, the request is handled in conformance with the organisation's standard procedures
Examples:
- request for information/advice/ documentation
- forgotten password.

Incident Management
- Incident detection and recording
- classification and initial support
- investigation and diagnosis
- resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking and communication

Additional Output
Reports and Audits

Service Level Management
- identifying customer requirements
- defining internal and external specifications
- agreeing contracts
- monitoring Service Levels
- management reporting
- evaluating process performance

Additional Output
Service Level Agreements (SLA)
Operational Level Agreements (OLA)
Underpinning Contracts (UC)
Service Level Requirements
Service Specifications
Service Quality Plan (SQP)
Service Catalogue
Service Achievement
Service-Level-Reports
Service Improvement Programme (SIP)
Reports and Audits

Financial Management
- Budgeting
- IT Accounting
- Charging
- Management reporting

To understand whether an IT organisation is doing the best that it can and to demonstrate this to its Customers, it has to both understand the true cost of providing a service and manage those costs professionally. To do this, it is usual to implement IT Accounting and Budgeting processes and often to implement Charging processes as well.

Additional Output
Budgets
Accounting System
Charging System
Pricing & Cost Models
Reports and Audits

Change Management
- Acceptance and filtering of RFCs
- Classification (category & priority)
- Approval (minimum: financial & technical feasability, business benefit)
- Authorization
- Chairing the CAB and the CAB/ Emergency Committee
- Planning and coordination
- Evaluation (PIR) and close of RFCs
- Management reporting

Additional Output
FSC
CAB minutes & actions
Reports and Audits

Manage urgent Changes

RFCs

Business Plans
Strategies, Requirements
Volumes

Business

IT Plans
Strategies

IT Manage-ment

Capacity Management

Business Capacity Management is responsible for ensuring that the future business requirements for IT Services are considered, planned and implemented in a timely fashion.

Service Capacity Management: The focus of this sub-process is the management of the performance of the live, operational IT Services used by the Customers. It is responsible for ensuring that the performance of all services, as detailed in the targets in the SLAs and SLRs, is monitored and measured, and that the collected data is recorded, analysed and reported. As necessary, action is taken to ensure that the performance of the services meets the business requirements. This is performed by staff with knowledge of all the areas of technology used in the delivery of end-to-end service, and often involves seeking advice from the specialists involved in Resource Capacity Management.

Resource Capacity Management: The focus in this sub-process is the management of the individual components of the IT Infrastructure. It is responsible for ensuring that all components within the IT Infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analysed and reported. In carrying out this work, the Capacity Management process is assisted by individuals with specialist knowledge in the particular areas of technology.

Additional Output
Capacity Plan
Baselines & Profiles
Thresholds & Alarms
Effectiveness Reports
Reports and Audits

Service Levels

FSC

Proactive Changes & Service Improvements

Incidents with details

Workarounds Resolutions

Known Errors

Workarounds Solutions

Updated Problem record

Problem Management
- **Problem Control**
  - Problem Identification & recording
  - Classification
  - Investigation & diagnosis
- **Error Control**
  - Error Identification & recording
  - Error assessment
  - Error resolution recording
  - Close (usually after PIR)
- **Proactive prevention of problems**
  - identifying trends
  - obtaining management information from Problem Management data
  - completion of major Problem reviews

Additional Output
Problem/Error Database
Trend Analysis
Reports and Audits

RFCs

Results
PIR

Other ITSM Processes

Adjustments

CMDB

IT Infrastructure Data - Configuration Management provides essential information about elements of the infrastructure, blueprints, hardware and software configurations, services, and other relationships such as 'is connected to', 'uses', and 'forms part of'.

The CAB, as defined in the Change Management process, with advice from Release Management, is responsible for recommending the content and scheduling of Releases. Release Management is then responsible for implementing the agreed Releases.
Release Management is normally represented on the CAB and is involved in establishing the organisation's Release policy. Although Release Management oversees the details of the roll out of a Change, it is under the control and authority of Change Management.

Change control - following tests and reviews and in response to day to day Changes, there is a need for the **ITSCM** plans to be updated. **ITSCM** must be included as part of the **Change Management** process to ensure that any Changes in the Infrastructure are reflected in the contingency arrangements provided by IT or third parties.

Proactive Changes & Service Improvements

Requirements for Availability, Maintainability and Reliability

Service Level Achievements

Incidents Problems

Incidents Problems

Incident Problem Management

SLA Breaches

SLA Breaches

Service Desk

Functionality Specification Cost

Technology

Products Services Cost

External Suppliers

Operational Schedules

Operations

Revised Schedules

Long term Deployment plans

Application Development

Recommendations

Dialog Change and Configuration Management Analysing impact, register changes

Availability Management
- determining the Availability requirements from the business for a new or enhanced IT Service and formulating the Availability and recovery design criteria for the IT Infrastructure
- in conjunction with ITSCM determining the vital business functions and impact arising from IT component failure. Where appropriate reviewing the Availability design criteria to provide additional resilience to prevent or minimise impact to the business
- defining the targets for Availability, reliability and maintainability for the IT Infrastructure components that underpin the IT Service to enable these to be documented and agreed within SLAs, OLAs and contracts
- establishing measures and reporting of Availability, Reliability and Maintainability that reflects the business, User and IT support organisation perspectives
- monitoring and trend analysis of the Availability, Reliability and Maintainability of IT components
- reviewing IT Service and component Availability and identifying unacceptable levels
- investigating the underlying reasons for unacceptable Availability.
- producing and maintaining an Availability Plan which prioritises and plans IT Availability improvements.

Additional Output
Availability Plan
Business Impact Assessment
Resilience and Risk Assessment
Thresholds and Alarms
Impact Analysis (CFIA, FTA, SOA)
Reports and Audits

Capacity Data

CDB

IT Service Continuity Management
- Initiation
- Requirements Analysis and Strategy Definition
- Implementation
- Operational Management
  - Education & Awareness
  - Review & Audit
  - Testing
  - Change Management
  - Training
  - Assurance

Additional Output
Policy
Business Impact Analysis
Risk Assessment
Business Continuity Strategy
Organisational Planning, Arrangements
Recovery Plan
Procedures
Reports and Audits

Special Roles
- ITSCM Manager
- BCM Board
- BCM Steering Committee
- Continuity Team Leaders and Members

AVM supports ITSCM by developing and implementing prevention measures.

Configuration Management
- Planning
- Identification
- Control
- Status accounting
- Verification and audit

Additional Output
CMDB
DSL
Policy & Standards
Reports and Audits

Remark
Ideally, Change Management should be regarded as an integral part of a Configuration Management system. However, because many installations have been practising Change Management without adopting full Configuration Management, the subject is treated separately.

Known Errors

Release Management
- Release policy and planning
- Release design, build and configuration
- Release acceptance
- rollout planning
- extensive testing to predefined acceptance criteria
- sign-off of the Release for implementation
- communication, preparation and training
- audits of hardware and software prior to and following the implementation of Changes
- installation of new or upgraded hardware
- storage of controlled software in both centralised and distributed systems
- Release, distribution and the installation of software

Additional Output
DHS
Release Policy
Release Plan
Documents for rollout (e.g. training material)
Reports and Audits

Whenever new versions of software are added to the DSL, its details should be simultaneously included in the CMDB. Similarly, whenever new or changed hardware is rolled out, the CMDB should be updated. The CMDB should always contain the current status information on all authorised software and hardware and is used to ensure that only the correct components are included in a Release.

DSL

SERVICES

Recommendations (Design for Availability / Recovery)

CAM and AVM are closely connected. Performance and capacity problems can result in the loss of the IT services. The customer may even consider poor performance to be equivalent to unavailability. Because of the many dependencies, the two processes need to be coordinated effectively. They both use many of the same tools and techniques such as Component Failure Impact Analysis (CFIA) and Fault Tree Analysis (FTA).

CAM specifies the minimum capacity needed to continue the service in the event of a disaster. The capacity needs of ITSCM should be constantly reviewed to ensure that they reflect day to day changes to the operating environment.

Steering

Business Continuity Management

Requirements

Business

Version 1.0.5 – Autor: Angelo Leisinger

Service Support Process

Service Delivery Process

activity

Role

information or result

© CLAVIS klw AG, CLAVISmap - ITIL® ist eine eingetragene Marke des OGC (Office of Government Commerce) - www.ogc.gov.uk.