

MATERNA
Information & Communications

ITIL® Version 3
Pocket Guide



IT's
value

Table of Contents

1	Management Summary	4
2	Service Strategy	8
2.1	Introduction	8
2.2	Service Strategy Processes	8
2.2.1	Financial Management & Return on Investment	8
2.2.2	Service Portfolio Management	9
2.2.3	Demand Management	9
3	Service Design	10
3.1	Introduction	10
3.2	Service Design Processes	10
3.2.1	Service Catalogue Management	10
3.2.2	Service Level Management	11
3.2.3	Capacity Management	11
3.2.4	Availability Management	12
3.2.5	IT Service Continuity Management	13
3.2.6	Information Security Management	13
3.2.7	Supplier Management	14
4	Service Transition	15
4.1	Introduction	15
4.2	Service Transition Processes	15
4.2.1	Transition Planning and Support	15
4.2.2	Change Management	16
4.2.3	Service Asset and Configuration Management	16
4.2.4	Release and Deployment Management	17
4.2.5	Service Validation and Testing	18

4.2.6	Evaluation	19
4.2.7	Knowledge Management	19
5	Service Operation	20
5.1	Introduction	20
5.2	Service Operation Processes	20
5.2.1	Event Management	20
5.2.2	Incident Management	21
5.2.3	Request Fulfilment	21
5.2.4	Problem Management	22
5.2.5	Access Management	23
5.3	Service Operation Functions	23
5.3.1	Service Desk	23
5.3.2	Technical Management	24
5.3.3	IT Operations Management	24
5.3.4	Application Management	24
6	Continual Service Improvement	25
6.1	Introduction	25
6.2	The 7 Step Improvement Process	25
7	ITIL®-compliant IT Service Management by MATERNA	27
7.1	Consulting, Implementation and accredited Training	27
7.2	The Company	29
8	Glossary	30

1 Management Summary

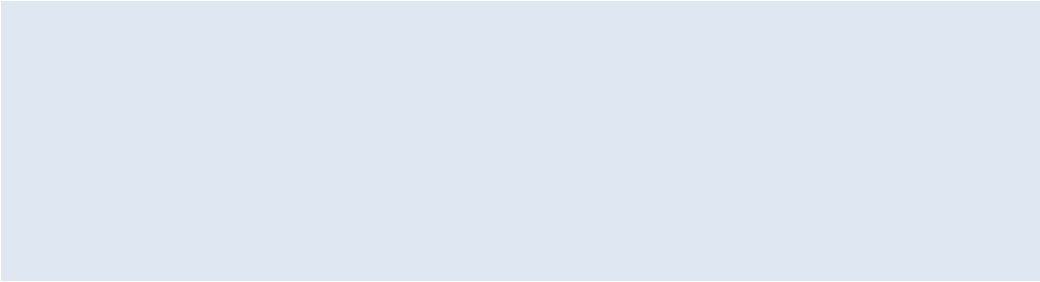
The success of a company is very much dependent on the quality of its IT infrastructure. Improving IT service quality while simultaneously standardising services and reducing costs generates a real competitive advantage.

The IT Infrastructure Library® (ITIL®) is a collection of specialist methodological principles for best practices with the purpose of establishing and improving service management capabilities like service processes, which leads to improved IT services and increases the value delivered to the customers. ITIL® was developed at the end of the '80s by the United Kingdom Office of Government Commerce (OGC) to optimise IT services within UK public administrations. In the meantime the ITIL® philosophy has gained international momentum in private industry and public administration. ITIL® services include training, certification, consulting, software and the appropriate implementation. ITIL® best practices are applicable to all types of organisations which provide services to businesses.

ITIL® is a framework, independent of manufacturers, that describes systematic procedures for the strategic positioning, design, introduction, transition, operation and improvement of IT services. ITIL® describes principles, processes, activities, functions as well as roles and responsibilities. This forms the basis for efficient and effective IT service management.

In June 2007, the current ITIL® version 3 was published, a necessary evolution of the well-known and widely implemented ITIL® version 2. Version 3 of ITIL® provides an improved structure and consistency, considers new technologies and has a strong alignment to ISO/IEC 20000. ISO/IEC 20000 provides a formal and universal standard for organisations seeking to have their service management capabilities audited and certified. While ISO/IEC 20000 is a standard to be aimed at and maintained, ITIL® V3 offers the body of knowledge for achieving this standard.

ITIL® is a registered trade mark of the Cabinet Office. IT Infrastructure Library® is a registered trade mark of the Cabinet Office.



IT service management means implementing and managing quality IT services that meet the needs of the business. It is performed by IT service providers by means of an appropriate mix of people, processes and technology. ITIL® V3 defines service management as a variety of specialised organisational capabilities for providing value to customers in the form of services. These capabilities for managing services throughout their lifecycle take the form of processes, which are sets of coordinated activities that produce the value creating outcomes, and functions. Both, therefore, are introduced in this pocket guide.

The main objectives for IT service management according to ITIL® are:

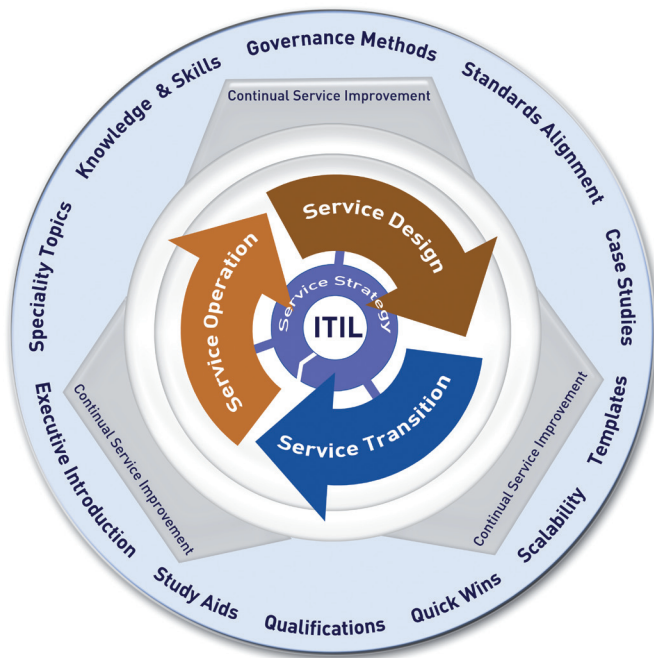
- The transformation of capabilities and resources of the service provider into value adding IT services.
- The orientation of IT services towards current and future requirements of the customer.
- Constant improvement to the quality of IT services together with long term constant or reduced costs.

The new ITIL® core consists of five publications. Each provides the guidance necessary for an integrated approach as required by the ISO/IEC 20000 standard specification. The five core publications are:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

The structure of the core is in the form of an interactive service lifecycle. Service Strategy represents policies and objectives and is the axis around which the lifecycle rotates. Service Design, Service Transition and Service Operation are progressive phases of the lifecycle that represent the design, introduction and ongoing operation, thereby implementing the Service Strategy. Continual Service Improvement focuses on learning and optimising. It supports companies in their efforts to derive improvement measures based on strategic objectives, to prioritise these and put them into practice. Therefore the service lifecycle is a comprehensive approach to service management.

The five core publications of ITIL® V3 are enhanced with a complementary set of publications with guidance specific to industry sectors, organisation types, operating models, and technology architectures. The ITIL® core provides structure, stability and strength for service management capabilities while the complementary guidance focuses on flexibility.



© Crown Copyright 2007. Reproduced under licence from OGC.

ITIL® provides best practice procedures but does not supply detailed instructions for their implementation and use. Support from qualified IT service management consultants is needed to adapt ITIL® processes to specific company conditions and to make them ISO/IEC 20000 compliant. In the following, the processes and functions of ITIL® V3 are introduced which build the service management capabilities of a service provider.

2 Service Strategy

2.1 Introduction

Service Strategy establishes an overall IT service management strategy. The processes of Service Strategy provide service providers with the ability to think and act in a strategic manner, i.e. to think about why something is done before thinking of how. Service Strategy and its processes increase the alignment between IT service management and the business strategies.

Service Strategy clarifies the following questions:

- What is our business and who is our customer?
- Which services need to be offered?
- How can we, as a service provider, differentiate ourselves from competitors?
- Which investments are beneficial?

2.2 Service Strategy Processes

2.2.1 Financial Management & Return on Investment

Financial Management brings transparency to the IT services and assets underlying the service provisioning. This facilitates targeted decision-making. The main tasks of Financial Management are financial planning (budgeting), the recording of service costs, service cost allocation, support of the portfolio management and investment analysis. The Return on Investment (ROI) process quantifies the value of an investment by calculating business cases and applies ROI methods.

Financial Management & Return on Investment clarifies the following questions:

- Is our differentiation strategy resulting in higher profits or revenues, lower costs, or greater service adoption?
- Which services cost us the most, and why?
- What are the volumes and types of consumed services, and what is the correlation to budget requirements?
- How efficient are our service provisioning models and where are our greatest service inefficiencies?
- What is the ROI of a potential investment?

2.2.2 Service Portfolio Management

Service Portfolio Management is responsible for the service portfolio, which is the complete set of services that are managed by a service provider, starting with the IT services of the service pipeline during the planning and development stage, and covers the productive IT services of the service catalogue, right through to the services which have already been deployed. The business needs and the service provider's response to those needs are aligned within this strategic process. The service portfolio is the key element for driving service strategies and managing service investments.

Service Portfolio Management clarifies the following questions:

- Why should customers buy such services?
- Why should customers buy such services from us?
- What are our strengths and weaknesses, opportunities and risks?
- How should our limited resources be allocated and distributed among the IT services?

2.2.3 Demand Management

The purpose of Demand Management is to measure and understand the customers' demand for services and to influence this according to the company's own capacity to meet these demands. Thus it is strongly linked to the Capacity Management which is described in Service Design. Demand Management techniques such as off-peak pricing, volume discounts and the creation of attractive service packages can actively influence service demand. This process is needed as poorly managed demand is a source of risk. Whilst excess capacity leads to unnecessary costs, a sudden spike in demand may catch the company unprepared and unable to deliver the services.

Demand Management clarifies the following questions:

- What is the demand for our services and how does it change over time?
- Which service packages and appropriate service level packages address the customers' demand?
- How can we actively influence the onset of demand to utilise our resources?

3 Service Design

3.1 Introduction

The best Service Strategy cannot be achieved without well designed services and service management processes. Service Design and its processes provide guidance for the design of innovative IT services which are suitable for the business or for its customers. This includes an assessment of the requisite architectures, processes, policies and documentation. The lifecycle phase Service Design is therefore essential for any IT service provider which wants to maximise its potential for meeting business objectives and creating added value for the business.

Service Design clarifies the following questions:

- How should we plan and design our services, architectures, processes, etc.?
- How can the risks and costs resulting from design flaws be reduced?
- How do we ensure that our services will perform as they are designed to do?

3.2 Service Design Processes

3.2.1 Service Catalogue Management

Service Catalogue Management provides a single source of consistent information about all of the agreed services and ensures that it is widely available to those who are approved to access it. The primary goal of Service Catalogue Management is to produce and maintain a service catalogue that contains accurate information about all operational services and those which are about to go live.

Service Catalogue Management clarifies the following questions:

- How do we define our services?
- Which information about our services is really valuable to our customers and how can we best present and provide them with this information?
- How do we ensure that the service catalogue is always reliable and up-to-date and that it is consistent with the service portfolio?

3.2.2 Service Level Management

Service Level Management (SLM) is responsible for negotiating, agreeing and documenting service level agreements (SLA) with the customers, and ensuring that these are met. It ensures that all IT service management processes, operational level agreements (OLA) and underpinning contracts (UC) are appropriate for the agreed service level targets. Monitoring, reporting and regular customer reviews are also tasks for SLM. It ensures that the performance is measured in a consistent, professional manner and that the services and the reports meet the needs of the business and customers. SLM establishes uniform communication channels and forms the interface for all service-related issues.

Service Level Management clarifies the following questions:

- How can we develop and improve the relationships with the customers?
- What are the concrete requirements of our customers and what service level targets should we agree with them?
- How do we ensure that the internal and external agreements, i.e. the OLAs and UCs, optimally support the attainment of the agreed service level targets?

3.2.3 Capacity Management

Capacity Management provides a point of contact for all capacity- and performance-related issues, relating both to IT services and the underlying resources. It ensures that cost-justifiable IT capacity always exists in all areas of IT and is matched to the current and future agreed needs of the business in a cost-effective manner. It thereby helps to deliver the agreed service level targets to the business. Hitches due to capacity shortfalls are avoided by defining thresholds and continually monitoring IT components.

Capacity Management clarifies the following questions:

- How do we plan our performance- and capacity-related IT resources and align them to the current and future needs of the business?
- How do we solve and prevent performance- and capacity-related incidents and problems?
- How can we optimise the utilisation of our capacity (e.g. with Demand Management techniques)?

3.2.4 Availability Management

Availability Management provides a point of contact for all availability-related issues and is responsible for defining, analysing, planning, measuring and improving all aspects of the availability of IT services. It ensures that the IT infrastructure and processes, tools, roles etc. are appropriate for the agreed service level targets for availability. This process thus acts so that the level of service availability is matched to or exceeds the current and future agreed needs of the customers in a cost-effective manner. Availability Management is important because availability and reliability of the IT services are highly visible to the customers and their users, and thus can directly influence customer satisfaction and the reputation of the service provider.

Availability Management clarifies the following questions:

- How do we plan the relevant IT resources in order to meet current and future business requirements?
- How do we ensure that we really can provide the level of availability agreed with the customer?
- How can availability and reliability be monitored and measured?

3.2.5 IT Service Continuity Management

IT Service Continuity Management (ITSCM) is responsible for managing any risks that could seriously impact on IT services and the supported business processes. It is based on the comprehensive Business Continuity Management (BCM) and the risks, effects and business requirements identified there. Preventive measures are initiated so as to avoid business-critical service breakdowns. By establishing plans and priorities for the quick resumption of the IT services, the risk of breakdown can be reduced to an acceptable level. This guarantees that the service provider can meet his obligation to provide the most essential agreed service levels, even in the event of a disaster, so that business can continue as usual.

IT Service Continuity Management clarifies the following questions:

- How do we put our continuity and recovery mechanisms in place to meet or exceed the agreed business continuity targets?
- What are the minimum business requirements and service levels?
- What are the relevant risks and resulting business impacts that have to be addressed in an IT service continuity plan?

3.2.6 Information Security Management

Information Security Management (ISM) ensures the confidentiality, integrity, availability and authenticity of an organisation's assets, information, data and IT services. It aligns information security with business security and ensures that security is effectively managed in all service management processes, activities, etc. This process forms the interface for all IT security issues and raises awareness among staff of the need for security within all IT services. A main task of ISM is to produce, maintain and enforce the information security policy.

Information Security Management clarifies the following questions:

- How do we ensure that information is available and usable when required?
- How do we ensure that information is observed by or disclosed to only those who have a right to know?
- How do we ensure that data, information and knowledge are complete, accurate and available?
- How should risk assessments, security tests, audits and reports be conducted?

3.2.7 Supplier Management

Supplier Management is responsible for ensuring that all contracts with suppliers, referred to as underpinning contracts (UCs), support the optimum provision of services by the service provider. To guarantee this, Supplier Management has to align the contracts with the SLAs agreed between the service provider and its customers. Supplier Management deals with contracts, monitors adherence to contractual obligations and manages the relationships to the suppliers.

Supplier Management clarifies the following questions:

- Are our supplier contracts aligned to the SLAs with our customers? Which targets should we bargain and agree on in contracts with our suppliers?
- How do we manage and control the performance of our suppliers?
- How do we manage the relationships with our suppliers according, among other things, to their importance (from the supplier of commodities to strategic)?

4 Service Transition

4.1 Introduction

Service Transition provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realised in Service Operation. The goal of Service Transition is to assist organisations seeking to plan and manage service changes and deploy service releases in the production environment successfully. Efficient and repeatable mechanisms are used to check whether the releases comply with the requirements. The processes of Service Transition fulfil a further elementary task: to provide information relating to all identified service assets and configuration items (CIs) for the entire service lifecycle and to keep this up to date.

Service Transition clarifies the following questions:

- How do we establish and maintain the integrity of all service assets?
- How do we plan, build, test and deploy the releases into production without adverse effects on the live environment?
- How do we store and present all the information about our service assets to provide relevant insight and knowledge for all processes within the service lifecycle?

4.2 Service Transition Processes

4.2.1 Transition Planning and Support

Transition Planning and Support is the process responsible for superior planning of the Service Transition phase and co-ordinating the capacity and resources the other Service Transition processes require. It ensures an integrated approach to all transition activities, e.g. planning and reporting to the appropriate stakeholders and decision-makers.

Transition Planning and Support clarifies the following questions:

- What is our overall transition strategy?
- How can our Service Transition plans be aligned?
- How should our resources for Service Transition be allocated?

4.2.2 Change Management

Every addition, modification or removal of anything that could have an effect on IT services is called a change – according to ITIL®. Change Management is responsible for controlling the lifecycle of all these changes. The primary objective is therefore to enable beneficial changes to be made, with as little disruption as possible to IT services. Change Management evaluates and coordinates requests for change (RFCs) so as to gear IT services more to business needs. Change Management ensures that standardised methods and procedures are used for efficient and prompt handling of all changes, thus minimising incidents and re-working. A Configuration Management System (CMS) supports the evaluation of RFCs and records all changes, e.g. to the IT infrastructure. This function also lies within the scope of the closely related field of Configuration Management.

Change Management clarifies the following questions:

- How do we reduce service disruptions caused by failed changes?
- How do we ensure that changes to service assets are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed?
- How do we meet governance, legal, contractual and regulatory requirements by providing transparency for all changes made to service assets?

4.2.3 Service Asset and Configuration Management

Service Asset and Configuration Management (SACM) is responsible for maintaining information about service assets and configuration items (CI) required for delivering IT services, including their relationships, throughout their lifecycle. A „service tree“ illustrates the relationship between services and the related hardware, software and network components, relevant documents, etc. This information is identified, maintained and controlled by the SACM before being stored in the configuration management system (CMS). In this way, it administrates all service assets and CIs throughout their lifecycle. SACM supports efficient and effective service management processes by providing accurate information and minimising the number of quality and compliance issues caused by improper configuration of services and assets.

Service Asset and Configuration Management clarifies the following questions:

- How do we maintain the integrity of service assets and CIs?
- How do we manage our service assets efficiently and effectively to support the other service management processes, in particular by delivering reliable and accurate information?
- How can we provide all the information about service assets and CIs in a central source, i.e. in a CMS?

4.2.4 Release and Deployment Management

A release is a collection of hardware, software, documentation, processes or other components required to implement one or more approved changes. Release and Deployment Management ensures that releases are planned, installed, tested, verified and/or deinstalled or withdrawn. It is responsible for the planning, scheduling and movement of releases to test and live environments and thereby ensures that the integrity of the live environment is protected. Deployment means finally moving releases to the live environment, also known as rollout. In this way the process guarantees that the necessary transfer of knowledge to customers, users and company and support staff really takes place.

Release and Deployment Management clarifies the following questions:

- How can approved changes be delivered faster, at optimum cost and with minimised risk?
- How do we provide consistency in the implementation approach?
- How do we contribute to auditable traceability through Service Transition?

4.2.5 Service Validation and Testing

Service Validation and Testing provides objective evidence that new or changed services will support the customer's business and stakeholder requirements, including the agreed service levels. It ensures that new or changed IT services match their design specifications and therefore deliver value to customers. Therefore issues, errors and risks within a release are to be identified, assessed and addressed within this process. So the main purpose of Service Validation and Testing is the quality assurance of a release, its components, the resultant service and service capability delivered by the release.

Service Validation and Testing clarifies the following questions:

- How do we eliminate errors or variances in service performance early in the service lifecycle to reduce the overall costs of a service throughout its lifecycle?
- How can we provide a measured degree of confidence that new or changed services will deliver the value and outcomes required of it?
- How can we provide a measured degree of confidence that the transition of new or changed services into operations will be successful and will not cause disruption to existing services?

4.2.6 Evaluation

Evaluation is responsible for assessing new or changed IT services to ensure that risks have been managed and to help determine whether to proceed with a change. It provides a consistent and standardised means of determining the performance of a change and supports the Change Management process with that information. Evaluation takes place during the deployment and before the final transition of a service into operations. It is based on reports created by Service Validation and Testing.

Evaluation clarifies the following questions:

- How can we determine the performance of a service change and what is the actual performance of a service change in comparison to the predicted one?
- Does a service change deliver the expected value to the customers?
- What are the risks associated with a service change?

4.2.7 Knowledge Management

Knowledge Management is responsible for gathering, analysing, storing and sharing knowledge and information within the organisation. It thus enables organisations to improve the quality of management decision-making by ensuring that reliable and secure information and data is available throughout the service lifecycle. Knowledge Management is responsible for the „service knowledge management system“ (SKMS), which is based on the configuration management system and further databases and tools.

Knowledge Management clarifies the following questions:

- Which data, information and knowledge should be recorded and shared?
- How do we finally generate usable knowledge from the gathered data?
- How do we transfer our knowledge to users, support staff, suppliers and other stakeholders?

5 Service Operation

5.1 Introduction

Service Operation provides guidance on achieving effectiveness and efficiency in the delivery and support of services by covering day-to-day management. Strategic objectives are ultimately realised through Service Operation, therefore making it a critical capability. The aim of Service Operation is to provide stability for the service delivery. This phase of the service lifecycle is also responsible for the ongoing management of the technology, which is mainly executed through functions like the Service Desk or Technical Management. From the customer's point of view, Service Operation is where the actual value is seen.

Service Operation clarifies the following questions:

- How do we finally conduct, control, measure and manage our services and processes that are planned by Service Design and implemented by Service Transition?
- Which ongoing, technology-based activities are necessary to deliver and support services?
- How do we handle our day-to-day operations to provide the most value to our customers?

5.2 Service Operation Processes

5.2.1 Event Management

An event is defined as a detectable occurrence that has significance for the management of the IT infrastructure or the delivery of IT services. The purpose of Event Management is to ensure that events are detected, understood and that appropriate actions are initiated. It is an entry point for the execution of many Service Operation processes and activities because it provides a basis for automating routine activities. Event Management also plays a key role in the early detection of incidents.

Event Management clarifies the following questions:

- How do we detect and generate notifications that are meaningful for the management of our IT infrastructure and IT service delivery?
- How do we proactively detect incidents to minimise their impact on the users?
- How do we automate operations by triggering their execution through events?

5.2.2 Incident Management

An incident is defined as an unplanned interruption to an IT service or a reduction in the quality of an IT service. Incident Management is responsible for managing the lifecycle of these incidents that are reported by the users through the Service Desk or logged/monitored by technical staff. The primary objective of Incident Management is to restore operations within SLA limits as quickly as possible and minimise the adverse impact on business operations. Incident Management and its outcomes are highly visible to the customers and for this reason it is one of the first processes to be implemented in service management projects.

Incident Management clarifies the following questions:

- How can we detect and solve incidents to minimise the downtime?
- How do we restore operations within SLA limits, as fast as possible?
- How should incidents be prioritised to meet the business requirements and service levels, i.e. which incidents should be handled first?

5.2.3 Request Fulfilment

Service request is used as a generic description for many different types of demand placed upon the IT department by the users. Typical service requests include the request to change or reset a password, to define access authorisations, to install additional software, to relocate or to provision new desktops. All of these are small changes with low risk that can be handled effectively and efficiently through this specialised process. Request Fulfilment provides a channel for users to request and receive standard services, information,

etc. and thereby relieves the Incident and Change Management processes that would have to handle these requests if a Request Fulfilment was not in place.

Request Fulfilment clarifies the following questions:

- How do we provide quick and effective access to standard services?
- How do we reduce the bureaucracy involved in requesting and receiving access to existing or new services?
- Which requests do our customers have?

5.2.4 Problem Management

ITIL® defines a 'problem' as the unknown cause of one or more incidents. Problem Management is responsible for managing the lifecycle of all problems. It proactively prevents problems and resulting incidents from happening, eliminates recurring incidents and minimises the impact of incidents that cannot be prevented. Thus there is a strong relationship between Incident and Problem Management and both processes typically use the same tools and similar categorisations, impact and priority coding systems to ease communication with each other. If a problem has been evaluated successfully, it is referred to as a „known error“. Problem Management is also responsible for maintaining all the information about problems and known errors, including identified workarounds, in the Known Error Database (KEDB).

Problem Management clarifies the following questions:

- How do we finally resolve our recurring incidents and thus increase productivity of users and support people?
- How do we increase the IT service availability and quality by proactively avoiding errors?
- How do we record, organise and provide information about identified resolutions (e.g. workarounds in a known error database)?

5.2.5 Access Management

Access Management is responsible for protecting the confidentiality, integrity and availability of the organisation's data and intellectual property by ensuring that only authorised users are able to access or modify the service assets. It provides the right for users to be able to use a service or group of services, while preventing access to non-authorised users and may also be needed for regulatory compliance reasons. Technologically, Access Management is usually executed by means of directory services.

Access Management clarifies the following questions:

- Who has access to what kind of data?
- How do we design and implement the right levels of access according to the security policy?
- How can we assure that access rights are removed when they are not needed any more (e.g. after the dismissal of an employee)?
- How do we manage multiple access rights for individual users effectively?

5.3 Service Operation Functions

The concept of functions refers to the people and automated measures that execute a process or an activity. Functions are units of organisations specialised in performing certain types of work. They are responsible for specific outcomes and are self-contained with capabilities and resources. The Service Desk is the most well-known and widely implemented function of ITIL® V2. The new functions of ITIL® V3 are Technical Management, IT Operations Management and Application Management.

5.3.1 Service Desk

The Service Desk is the single point of contact (SPOC) for users to report a service disruption or place a service request. Its functions include aspects of the two processes of Incident Management and Request Fulfilment. Therefore it is an important component for IT service providers because it handles all

incidents and service requests on a day-to-day basis. That is why the Service Desk is the key element for ensuring customer satisfaction. It not only provides a central point of communication to the users but also an internal point of coordination for several IT groups and processes.

5.3.2 Technical Management

Technical Management provides detailed technical skills and resources needed to support the ongoing operation of the IT infrastructure. It also plays an important role in the design, testing, release and improvement of IT services. Technical Management departments (e.g. mainframe, server, network) can also be responsible for the daily operation of sub-sections of the IT infrastructure.

5.3.3 IT Operations Management

IT Operations Management is the function responsible for the daily operational activities needed to manage the IT infrastructure. This is done according to the performance standards defined during Service Design. IT Operations Management has two functions that are unique and which are generally formal organisational structures.

These are:

- **IT Operations Control**, which is generally staffed by shifts of operators and which ensures that routine operational tasks are carried out. These include monitoring, job scheduling, backups and maintenance work.
- **Facilities Management**, which refers to the management of the physical IT environment, usually data centres or computer rooms.

5.3.4 Application Management

Application Management is responsible for managing and supporting applications throughout their lifecycle and also plays an important role in the design, testing and improvement of applications. Application Management is to applications what Technical Management is to the IT infrastructure. It is usually divided into departments based on the application portfolio.

6 Continual Service Improvement

6.1 Introduction

Continual Service Improvement (CSI) is responsible for improvements to the services which support the customer's business processes, the underlying processes and the overall ITSM service lifecycle. CSI thereby aligns or realigns IT services, processes, etc. to the changing business requirements. CSI is based on the continual measurement of the performance. The improvements are made to processes, IT services and IT infrastructure in order to increase their efficiency and effectiveness. CSI provides instrumental guidance in creating and maintaining value for customers through better design, introduction and operation of services. CSI is not a project but an ongoing activity. The basic process of CSI is the 7 Step Improvement Process, which is supported by Service Measurement and Service Reporting. Other methods can also be applied in CSI, such as the Deming Cycle, well-known even outside the field of ITIL®. This consists of the phases Plan, Do, Check and Act (PDCA cycle).

Continual Service Improvement clarifies the following questions:

- How do we improve the service quality on a continual basis?
- How do we increase the value our IT services create?
- How do we improve process effectiveness and/or efficiency?

6.2 The 7 Step Improvement Process

Step 1: Define what you should measure

By talking to the customers and the IT management a list should be compiled of what is important to measure. Vision and mission statements, the service catalogue, service level requirements and targets, etc. can be used as input for this first step.

Step 2: Define what you can measure

Every organisation has limitations on what they can actually measure. What cannot be measured should not appear in SLAs. The reports already created and tools used by an organisation should be the starting point for identifying

what can already be measured or what can be measured with reasonable effort, e.g. by (re-)configuring the tools.

Step 3: Gathering the data

Gathering data requires a form of monitoring to be in place. The data collection should gather technology metrics, process metrics as well as service metrics. Important questions to answer in this step are who is responsible for collecting the data and how often it should be carried out.

Step 4: Processing the data

The task of this fourth step is to process the data from multiple disparate sources into a valid comparison and in the required format. After this the data is aligned, rationalised and accuracy is evaluated, so that analysis can then be started.

Step 5: Analysing and evaluating the data

This fifth step of the improvement process identifies weak spots in the IT services and processes as well as trends and the impact on the business, then devises corrective action. The result of this step 5 is a conclusion on how to proceed.

Step 6: Presenting and using the information

In this sixth step the knowledge generated by the previous steps is presented to the business in a form and manner that reflects their needs and assists them in determining and deciding on how to continue. This step communicates the answers to the “Did we get there?” question.

Step 7: Implementing corrective action

Corrective action means using the knowledge to optimise, improve and correct services. Communicating and explaining the corrective action to the organisation is also part of this final step in the 7 Step Improvement Process.

7 ITIL®-compliant IT Service Management by MATERNA

7.1 Consulting, Implementation and accredited Training

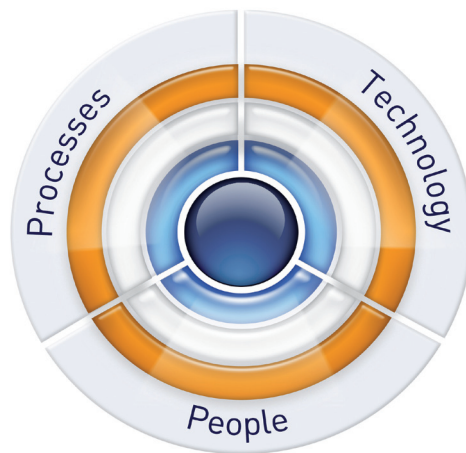
MATERNA has been designing successful IT service management solutions for many years. The result is a sound, cross-sector knowledge of processes and organisational structures for the optimised planning, provision and monitoring of IT services. We offer a comprehensive portfolio of services in the field of implementation and optimisation of IT service management processes. These include management workshops, service excellence assessments, planning, consulting and implementation services, not to mention an extensive range of training courses, all from one source. For the analysis, consulting and implementation of ITSM processes and technologies, MATERNA successfully applies the tried-and-tested ITIL® guidelines. ITIL® allows you to continuously review and optimise your IT processes.

Staff training is the key factor for successful IT management initiatives – both in technology and process-oriented projects. That is why MATERNA’s portfolio comprises ITIL® training courses, ITIL® simulations, ISO 20000 and product training courses. The training programmes are offered as standard seminars, tailored training courses on site or as a component of larger technology projects and ISO 20000 certifications.

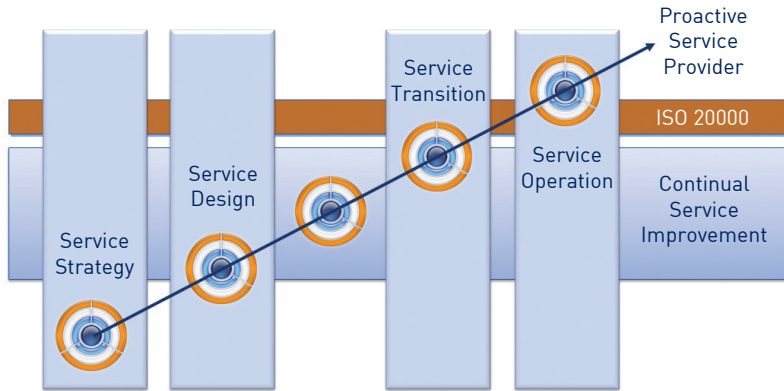


ITIL® is a registered trade mark of the Cabinet Office. IT Infrastructure Library® is a registered trade mark of the Cabinet Office. The Swirl logo™ is a trade mark of the Cabinet Office.

Furthermore, the ISO 20000 industry standard makes it possible to measure objectively and to certify IT service management on the basis of internationally applicable standards. Within the framework of a service excellence assessment (an assessment of the current situation) we analyse the conformity of your IT service processes and accompany IT companies on the route to attaining the international quality standard ISO 20000 and the follow-up audits.



“Service Excellence“ is MATERNA’s consulting method for a strategically positioned and value-added IT. “Service Excellence” is more than just a technically oriented approach. This consulting method takes into account all of the essential elements for high service quality: processes, organisation and technologies.



The route to "Service Excellence" consists of five disciplines and various levels of maturity.

7.2 The Company

MATERNA is a leading, independent IT service provider. You will find us at various locations throughout Germany and in a number of European countries. For 30 years we have been active players in the markets of information and communication technology. Our customers include many large corporations and SMEs, as well as numerous public administrations. MATERNA offers solutions for the optimisation of IT-supported business processes in the segments of IT management, business applications and specialised applications for public administration. The service package consists of the modules process and technology consulting, planning, implementation, integration, maintenance and training.

8 Glossary

Change	Every addition, modification or removal of anything that could have an effect on IT services.
Configuration Item (CI)	Any asset, component or other item that needs to be managed by Configuration Management in order to deliver IT services. Information about each CI is recorded in a configuration record. CIs typically include IT services, hardware, software, documentation, etc.
Configuration Management Database (CMDB)	A database used to store configuration on records of all configuration items throughout their lifecycle. The configuration management system maintains one or more CMDBs.
Configuration Management System (CMS)	A set of tools and databases that are used to manage an IT service provider's configuration data. The CMS includes tools for collecting, storing, managing, updating and presenting data about all configuration items and their relationships.
Event	A change of state that has significance for the management of the IT infrastructure or the delivery of a service. An event e.g. can be a means for alerting IT operations personnel to take actions.
Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service.

IT Service Continuity Plan	A contingency plan describing the procedures that have to be followed to recover IT services in the case of a serious service disruption.
Known Error	A problem that has a documented root cause and a workaround.
Operational Level Agreement (OLA)	An agreement between an IT service provider and another part of the same organisation that supports the delivery of services. Service level targets within the OLAs are to support the ones defined in the SLAs with the customers.
Problem	An unknown cause of one or more incidents.
Release	A collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT services.
Request for Change (RFC)	A formal proposal for a change to be made, which includes details of the proposed change.
Service	A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific cost and risks.
Service Asset	Any resource or capability that contributes to the delivery of a service. There are nine types of service assets: management, organisation, process, knowledge, information, applications, infrastructure, financial capital and people.

Service Catalogue	A database or structured document with complete information about all IT services. It is the only part of the service portfolio that is visible to the customers and contains deliverables, prices, etc.
Service Knowledge Management System (SKMS)	A set of tools and databases used to manage all the information and knowledge a service provider needs to manage the lifecycle of its services. The SKMS includes the configuration management system.
Service Level Agreement (SLA)	An agreement between an IT service provider and a customer, describing the IT service, the service level targets, responsibilities, etc.
Service Level Target	A measurable commitment that is documented in a service level agreement which specifies the customer's requirements for a service.
Service Portfolio	The complete set of services managed by the IT service provider. It includes three parts: the service pipeline (proposed or currently developed services), the service catalogue (available services) and the retired services.
Service Request	A request from a user for information, for access to a new IT service (e.g. a file service), for a standard change (e.g. installing software on the user's desktop) or other matters like a password reset, etc.

Single Point of Contact (SPOC)	The central contact point for users to report errors, to receive help with the use of a service, etc.
Underpinning Contract (UC)	A contract between an IT service provider and a third party supplier, which provides goods to support the delivery of services to the customers. Service level targets within the UCs are to support the ones defined in the SLAs with the customers.
Workaround	Reducing or eliminating the impact of incidents or problems for which a full resolution is not yet available. For example by restarting a failed configuration item.

ITIL® is a registered trade mark of the Cabinet Office. IT Infrastructure Library® is a registered trade mark of the Cabinet Office. The Swirl logo™ is a trade mark of the Cabinet Office.

Notes

Notes

MATERNA

Information & Communications

marketing@materna.com

www.materna.com