Standards for lightweight
IT service management

Part 0: Overview and vocabulary

Edition 2022 – Version 3.0

This work is licensed under a Creative Commons
Attribution 4.0 International License.
www.fitsm.eu

Document control

Document title	Part 0: Overview and vocabulary
Document version	3.0
Release date	2022-02-04

Table of Contents

1. Foreword 1

2. About this document 1

3. Key principles for IT service management and FitSM 2

3.1 Foundation for systematic IT service management 2

3.2 The FitSM approach to managing IT services 2

4. Overview of the FitSM family of standards 3

5. Overview of the FitSM process model 3

6. Terms and definitions 5

6.1 Activity 5

6.2 Assessment 5

6.3 Audit 5

6.4 Availability 5

6.5 Availability of information 5

6.6 Capability level 6

6.7 Capacity 6

6.8 Change 6

6.9 Classification 6

6.10 Closure 6

6.11 Competence 6

6.12 Confidentiality of information 6

6.13 Conformity 6

6.14 Configuration 7

6.15 Configuration item (CI) 7

6.16 Configuration management database (CMDB) 7

6.17 Continuity 7

6.18 Customer 7

6.19 Demand 7

6.20 Document 8

6.21 Effectiveness 8

6.22 Efficiency 8

FitSM was co-funded by the European Commission under contract number 312851.

6.23 Emergency change ... 8
6.24 Escalation ... 8
6.25 Federation ... 8
6.26 Federation member ... 8
6.27 Federator ... 8
6.28 Improvement ... 9
6.29 Incident ... 9
6.30 Information security ... 9
6.31 Information security control ... 9
6.32 Information security event ... 9
6.33 Information security incident ... 9
6.34 Integrity of information ... 9
6.35 IT service ... 9
6.36 IT service management (ITSM) ... 9
6.37 Key performance indicator (KPI) ... 9
6.38 Known error ... 10
6.39 Major change ... 10
6.40 Major incident ... 10
6.41 Management review ... 10
6.42 Management system ... 10
6.43 Maturity level ... 10
6.44 Nonconformity ... 10
6.45 Operational level agreement (OLA) ... 11
6.46 Operational target ... 11
6.47 Policy ... 11
6.48 Post implementation review (PIR) ... 11
6.49 Priority ... 11
6.50 Problem ... 11
6.51 Procedure ... 11
6.52 Process ... 11
6.53 Record ... 12
6.54 Release ... 12
6.55 Release and deployment strategy ... 12
6.56 Request for change (RFC) ... 12
6.57 Risk ... 12
6.58 Role ... 12

FitSM was co-funded by the European Commission under contract number 312851.

6.59 Service 12
6.60 Service acceptance criteria (SAC) 12
6.61 Service catalogue 13
6.62 Service component 13
6.63 Service design and transition 13
6.64 Service level agreement (SLA) 13
6.65 Service management 13
6.66 Service management plan 13
6.67 Service management system (SMS) 14
6.68 Service portfolio 14
6.69 Service provider 14
6.70 Service report 14
6.71 Service request 14
6.72 Service review 14
6.73 Service target 14
6.74 Supplier 14
6.75 Top management 15
6.76 Underpinning agreement (UA) 15
6.77 Underpinning contract (UC) 15
6.78 User 15
6.79 Value 15
6.80 Workaround 15

1. Foreword

FitSM is a lightweight standards family aimed at supporting the implementation of IT service management (ITSM), including federated scenarios. The FitSM approach is built on four key principles: practicality, consistency, sufficiency and extendibility.

FitSM is and will remain free for everybody. This covers all parts of the standard, including the core parts and implementation aids. All parts of the FitSM standard and related material published by the FitSM working group are licensed under a Creative Commons International License.

The development of FitSM was supported by the European Commission as part of the Seventh Framework Programme. FitSM is owned and maintained by ITEMO e.V., a non-profit partnership of specialists in the field of IT management, including experts from industry and research.

FitSM is designed to be compatible with the International Standard ISO/IEC 20000 and the IT Infrastructure Library (ITIL). However, the FitSM process model, requirements, recommended activities and role model target a lightweight and more achievable implementation. The FitSM family is made up of several documents, providing guidance and input on different aspects of ITSM:

- FitSM-0: Overview and vocabulary (this document)
- FitSM-1: Requirements
- FitSM-2: Process activities and implementation
- FitSM-3: Role model
- FitSM-4: Selected templates and samples *(set of documents under continual development)*
- FitSM-5: Selected guides *(set of documents under continual development)*
- FitSM-6: Maturity and capability assessment scheme

All documents are available and published in their most recent version through the website www.fitsm.eu. Enquiries about the standard and its applicability should be directed by e-mail to info@fitsm.eu.

2. About this document

This part of FitSM provides an overview of the FitSM family and a common vocabulary used by the other parts of the standard (in particular by FitSM-1). It helps to harmonise and facilitate discussion by those trying to implement IT Service Management using FitSM or any other compatible ITSM approach.

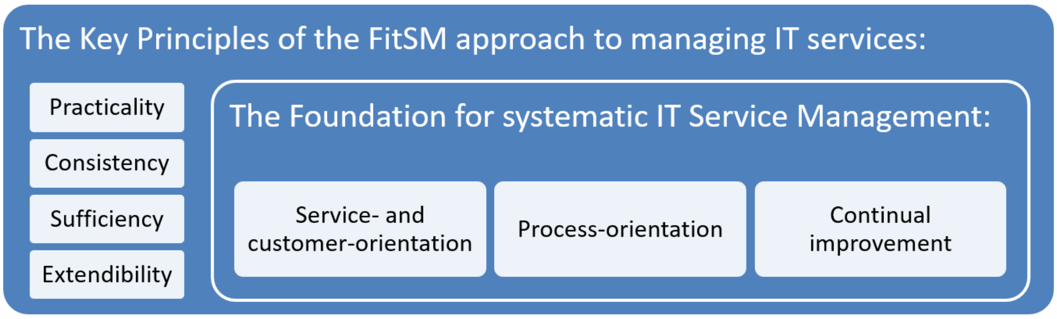
This part of the standard provides:

- an overview of the key principles behind ITSM and FitSM;
- a general overview of the FitSM family of standards;
- an overview of the FitSM process model;
- terms and definitions for use in the FitSM family of standards.

This standard is applicable to all types of organisation (e.g. commercial enterprises, government agencies, non-profit organizations) from which IT services are provided, regardless of type, size and the nature of the services delivered.

3. Key principles for IT service management and FitSM

Seven simple principles stand for the key ideas behind ITSM and the spirit of FitSM.


The Key Principles of the FitSM approach to managing IT services:
Practicality
Consistency
Sufficiency
Extendibility
The Foundation for systematic IT Service Management:
Service- and customer-orientation
Process-orientation
Continual improvement

3.1 Foundation for systematic IT service management

The first three principles reflect the main ideas behind ITSM as pursued by many organisations providing IT services.

Principle	Explanation
Service- and customer-orientation	Business-supporting IT provided to customers and users is subject to services with clearly defined service levels. The service portfolio is well-understood by the service provider and aligned to the needs and expectations of (potential) customers. Both the service provider and customer are aware of the agreed service targets.
Process-orientation	Activities required to plan, deliver, operate and control services are carried out as part of well-understood processes. *The reference process model that builds the foundation for the FitSM standard is introduced in section 5 of this document.*
Continual improvement	The entire service management system follows the plan-do-check-act approach. All processes and activities necessary to manage IT services as well as the services themselves are subject to evaluation, aiming at identifying opportunities for improvement and taking adequate follow-up action.

3.2 The FitSM approach to managing IT services

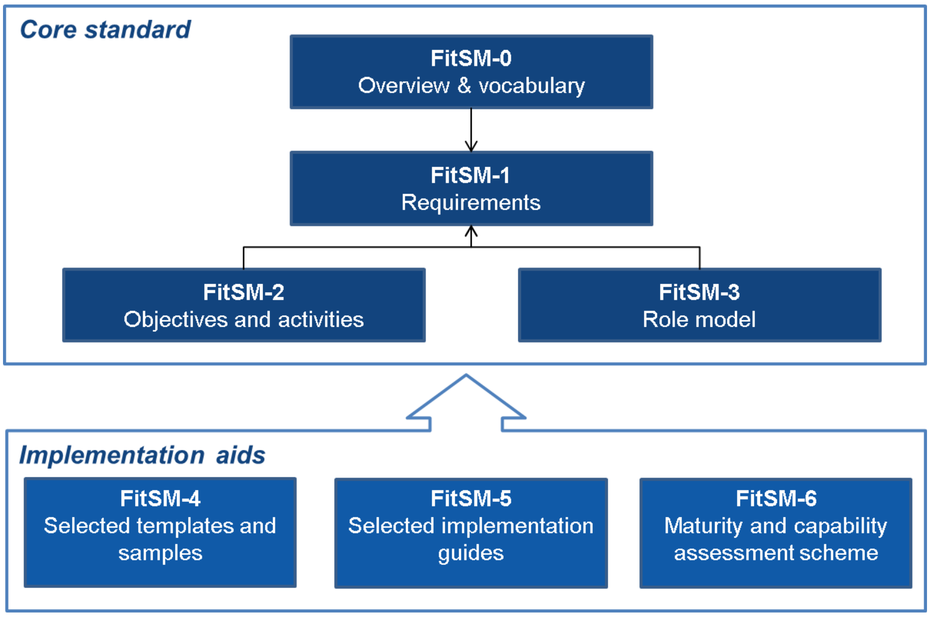
In the world of IT service management, FitSM is a unique standard. It is designed towards supporting the implementation of ITSM according to these four key principles.

Principle	Explanation
Practicality	Good enough and working is better than perfect and perpetually in planning.

Consistency	Assigning roles and making sure that activities are performed consistently is the first priority. Optimisation and detailed documentation are great, but they come later.
Sufficiency	Define and deploy parts of your Service Management System as they are needed. Not all processes, documents and other elements are needed on day one.
Extendibility	Starting small lets you build up capability and draw in other sources of knowledge as needed.

4. Overview of the FitSM family of standards

The FitSM family is made up of several documents, providing guidance and input on different aspects of ITSM. The following figure shows their relationships.


Core standard
FitSM-0
Overview & vocabulary
FitSM-1
Requirements
FitSM-2
Objectives and activities
FitSM-3
Role model
Implementation aids
FitSM-4
Selected templates and samples
FitSM-5
Selected implementation guides
FitSM-6
Maturity and capability assessment scheme

5. Overview of the FitSM process model

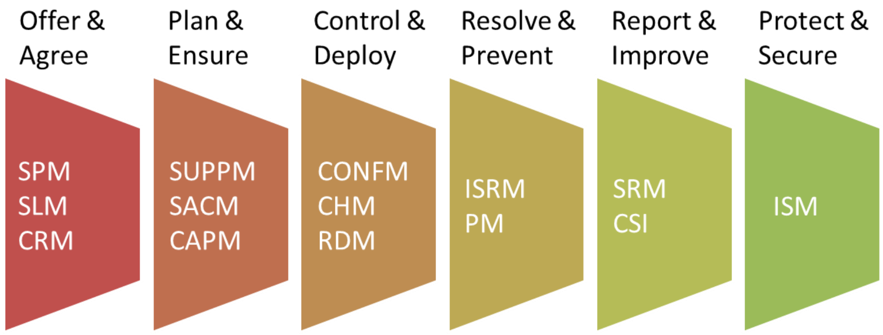
All parts of FitSM are based on an understanding of the following 14 core processes for IT service management (ITSM).

Process	Objective
Service portfolio management (SPM)	To define and maintain the service portfolio
Service level management (SLM)	To maintain a service catalogue, and to define, agree and monitor service levels with customers by establishing meaningful service level agreements (SLAs) and supportive operational level agreements (OLAs) and underpinning agreements (UAs) with suppliers

Service reporting management (SRM)	To specify all service reports and ensure they are produced according to specifications in a timely manner
Service availability and continuity management (SACM)	To ensure sufficient service availability to meet agreed requirements and adequate service continuity
Capacity management (CAPM)	To ensure sufficient capacities are provided to meet agreed service capacity and performance requirements
Information security management (ISM)	To manage information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information are preserved
Customer relationship management (CRM)	To establish and maintain a good relationship with customers receiving services
Supplier relationship management (SUPPM)	To establish and maintain a healthy relationship with internal and external suppliers supporting the service provider in delivering services to customers, and monitor their performance
Incident and service request management (ISRM)	To restore normal / agreed service operation within the agreed time after the occurrence of an incident, and to respond to user service requests
Problem management (PM)	To investigate the root causes of (recurring) incidents in order to avoid future recurrence of incidents by resolving the underlying cause, or to ensure workarounds / temporary fixes are available
Configuration management (CONFM)	To provide and maintain a logical model of all configuration items (CIs) and their relationships and dependencies
Change management (CHM)	To ensure changes to CIs are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services
Release and deployment management (RDM)	To bundle changes of one or more CIs to releases, so that these changes can be tested and deployed to the live environment together
Continual service improvement management (CSI)	To identify, prioritize, plan, implement and review improvements to services and service management

For each of these processes, as well as for a number of general aspects in the context of ITSM, FitSM-1 defines a small number of implementation requirements, while FitSM-2 provides guidelines on the activities to set up and implement ITSM using these processes. FitSM-3 describes the proposed roles to be assigned to execute the ITSM processes as part of a service management system.

The following figure shows a possible grouping of the FitSM processes, based on six main topic areas.



6. Terms and definitions

For the purpose of the FitSM family of standards, the following terms and definitions apply.

6.1 Activity

Set of actions carried out within a *process*

6.2 Assessment

Set of actions to evaluate the *capability level* of a *process* or the overall *maturity level* of a *management system*

6.3 Audit

Systematic, independent and documented *process* for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1: Audit evidence is typically based on documented information, information provided during an audit interview, and information gathered through observation.

Note 2: Audit criteria may be based on requirements from a *management system* (including *policies*, *processes* and *procedures*), agreements (including *service level agreements* and *underpinning agreements*), contracts, standards or legislation.

Note 3: An audit may be an internal audit, if it is conducted under the direct responsibility of the organisation or *federation* that is subject to the audit, or an external audit, if it is conducted by an external party.

Note 4: Both internal and external audits should be conducted by skilled and experienced auditors, and auditors should not audit their own work or areas of responsibilities to ensure the impartiality of the results.

6.4 Availability

Ability of a *service* or *service component* to fulfil its intended function at a specific time or over a specific period of time

6.5 Availability of information

Property of information being available to and usable by an authorized party

Note: Availability of information may also be referred to as *accessibility of information*.

6.6 Capability level

Achieved level of *effectiveness* of an individual *process* or general aspect of management

6.7 Capacity

Maximum extent to which a certain element of the infrastructure (such as a *configuration item*) can be used

Note: This might mean the total disk capacity or network bandwidth. It could also be the maximum transaction throughput of a system.

6.8 Change

Alteration (such as addition, removal, modification, replacement) of a *configuration item (CI)*

6.9 Classification

Assignment of items to defined groups based on common attributes, relations or other criteria

Note 1: Items that are subject to classification may include *documents*, *records* (such as *incident records* or *change records*), *services*, *configuration items (CIs)*, etc. Defined groups may include categories (such as *incident* categories or *change* categories) or *priority* levels.

Note 2: The act of classification often comprises the application of more than one classification scheme. For instance, an *incident record* might be assigned to a technical *incident* category such as ‘software related’, ‘network related’, etc., and also to a *priority* level like ‘low priority’, ‘medium priority’, etc. The assignment of various *incidents*, *service requests*, *changes* and *problems* to an affected *CI* is also a classification.

Note 3: Besides the presentation and analysis of relationships, classification is often used as input for controlling the workflow of a *process*, e.g. by assigning a *priority* level to an *incident*.

6.10 Closure

Final *activity* in a workflow of a *process* to indicate no further action is required for a specific case

Note: Cases that are subject to closure may include *incidents, problems, service requests or changes*. The *activity* of closure puts the connected *record* (such as the *incident record*, *problem record*, *service request record* or *change record*) in its final status, usually called ‘closed’.

6.11 Competence

Sum of knowledge, skills and experience that an individual or group needs to effectively take on a specific *role*

6.12 Confidentiality of information

Property of information not being *accessible* to unauthorized parties

6.13 Conformity

Extent to which requirements are met in some context

Note: In the context of FitSM, the term compliance is generally used as a synonym for conformity. However, sometimes conformity is used in the context of adherence to internal regulations and requirements as defined by *policies*, *processes* and *procedures*, while compliance is used in the context of adherence to external requirements, such as laws, standards and contracts.

6.14 Configuration

State of a specified set of attributes, relationships and other relevant properties of one or more *configuration items (CIs)*

Note: The documented configuration of a number of CIs at a given point in time is called a configuration baseline, which is usually taken prior to the deployment of one or more *changes* to these CIs in the live environment.

6.15 Configuration item (CI)

Element that contributes to the delivery of one or more *services* or *service components*, therefore requiring control of its *configuration*

Note 1: CIs can vary widely, from technical components (e.g. computer hardware, network components, software) to non-technical items such as *documents* (e.g. *service level agreements*, manuals, license documentation).

Note 2: The data necessary for effective control of a CI is stored in a CI *record*. In addition to attributes of the CI, the CI *record* likely includes information on relationships it has with other CIs, *service components* and *services*. CI *records* are stored in a *configuration management database (CMDB)*.

6.16 Configuration management database (CMDB)

Store for data about *configuration items (CIs)*

Note: A CMDB is not necessarily a single database covering all *configuration items (CIs)*. It may rather be composed of multiple physical data stores.

6.17 Continuity

Property of a *service* to maintain all or parts of its functionality, even in exceptional circumstances

Note: Exceptional circumstances include emergencies, crises or disasters which affect the ability to provide *services* over extended periods of time.

6.18 Customer

Organisation or part of an organisation that commissions a *service provider* in order to receive one or more *services*

Note: A customer usually represents a number of *users*.

6.19 Demand

Potential or identified desire of *customers* for a *service*

6.20 Document

Information and its supporting medium

Note: Examples of documents include *policies*, plans, *process* descriptions, *procedures*, *service level agreements*, contracts or *records* of *activities* performed.

6.21 Effectiveness

Extent to which goals and expectations are met

Note: In a *management system*, effectiveness is mostly measured against the defined goals of the *processes* that are subject to this system.

6.22 Efficiency

Degree of ability to meet goals and expectations with minimum consumption of resources

Note 1: In a *management system*, efficiency is mostly considered in the context of the *processes* that are subject to this system.

Note 2: Resources may be human, technical, informational or financial.

6.23 Emergency change

Change with a very high urgency to being implemented in order to avoid negative consequences

6.24 Escalation

Change of responsibility for a case (such as an *incident, service request*, *problem* or *change*) or *activity* to another individual or group

Note: There are two basic types of escalation: Hierarchical escalation transfers responsibility (temporarily) to someone with a higher level of authority. Functional escalation transfers responsibility to someone with a different set of *competencies* or privileges required to handle the case or activity.

6.25 Federation

Situation in which multiple parties, the *federation members*, jointly contribute to the delivery of *services* to *customers* without being organised in a strict hierarchical setup or supply chain.

6.26 Federation member

Individual, organisation or body that works together with other federation members in a *federation* to provide one or more *services*

Note: Often, federation members will not be bound together by strict contractual agreements.

6.27 Federator

Body that acts to coordinate a set of *federation members*

6.28 Improvement

Action or set of actions carried out to increase the level of *conformity*, *effectiveness* or *efficiency* of a *management system*, *process* or *activity*, or to increase the quality or performance of a *service* or *service component*

Note: An improvement is usually implemented after an opportunity for improvement has been identified, for instance during a *service review*, *audit* or *management review*.

6.29 Incident

Unplanned disruption of operation in a *service* or *service component,* or degradation of service quality versus the expected or agreed service level or operational level according to *service level agreements (SLAs)*, *operational level agreements (OLAs)* and *underpinning agreements (UAs)*.

6.30 Information security

Preservation of *confidentiality*, *integrity* and *accessibility* of information

6.31 Information security control

Means of controlling or treating one or more *risks* to *information security*

6.32 Information security event

Occurrence or previously unknown situation indicating a possible breach of *information security*

Note: An occurrence or situation is considered a potential breach of *information security* if it may lead to a negative impact on the *confidentiality*, *integrity* and / or *accessibility* of one or more information assets.

6.33 Information security incident

Single *information security event* or a series of *information security events* with a significant probability of having a negative impact on the delivery of *services* to *customers*, and therefore on the *customers'* business operations

6.34 Integrity of information

Property of information not being subject to unauthorized modification, duplication or deletion

6.35 IT service

Service that is enabled by the use of information technology (IT)

6.36 IT service management (ITSM)

Entirety of *activities* performed by an IT *service provider* to plan, deliver, operate and control *IT services* offered to *customers*

Note: The *activities* carried out in the ITSM context should be directed by *policies* and structured and organised by *processes* and supporting *procedures*.

6.37 Key performance indicator (KPI)

Metric that is used to track the performance, *effectiveness* or *efficiency* of a *service* or *process*

Note: KPIs are generally important metrics that will be aligned to critical success factors and important goals. KPIs are therefore a subset of all possible metrics, intended to allow for monitoring a *service* or *process*.

6.38 Known error

Problem which has not (yet) been corrected, but for which there is a documented workaround or temporary fix to prevent (excessive) negative impact on *services*

6.39 Major change

Change that (may) have a significant impact on one or more *services*

6.40 Major incident

Incident that (may) have significant impact on the *customer*

6.41 Management review

Periodic evaluation of the suitability, *maturity* and *efficiency* of the entire *management system* by its accountable owner(s), from which opportunities for *improvement* are identified and follow-up actions are determined

Note: The accountable owner of a *management system* is usually a *top management* representative of the organisation operating the *management system*. In a *federation*, the accountable owner is usually one person nominated by *top management* representatives of all organisations (i.e. *federation members*) involved.

6.42 Management system

Entirety of *policies*, *processes*, *procedures* and related resources and capabilities aiming at effectively performing management tasks in a given context and for a given subject

Note 1: A management system is generally intangible. It is based on the idea of a systematic, structured and *process*-oriented way of managing.

Note 2: While documentation (such as *process* definitions, *procedures* and *records*) and tools (such as workflow support and monitoring tools) can be parts of a management system, management system considerations are not limited to the questions of documentation and tool support.

Note 3: With respect to *(IT) service management* and the FitSM standard series, the idea of a *service management system (SMS)* is a central concept, where the context of the management system is the organisational context of the *service provider*, and the subject is to plan, deliver, operate and control *(IT) services*.

6.43 Maturity level

Achieved overall *effectiveness* of a *service management system*, based on the combination of the *capability levels* of its processes and general aspects of management

6.44 Nonconformity

Case or situation where a requirement is not fulfilled

Note: This may also be referred to as noncompliance.

6.45 Operational level agreement (OLA)

Documented agreement between a *service provider* and an internal *supplier* that specifies the underpinning *service(s)* or *service component(s)* to be provided by the internal *supplier* or *federation member*, together with the related *service targets*

Note: In a *federation*, OLAs may be agreed between the *federator* and *federation members*.

6.46 Operational target

Reference / target value for a parameter used to measure the performance of a *service component*, listed in an *operational level agreement (OLA)* or *underpinning agreement (UA)* related to this *service component*

Note: Typical operational targets might include *availability* or allowed resolution times for *incidents.*

6.47 Policy

Documented set of intentions, expectations, goals, rules and requirements, often formally expressed *by top management* representatives in an organisation or *federation*

Note: Policies are then realised in *processes*, which are in turn made up of *activities* that people carry out according to defined *procedures.*

6.48 Post implementation review (PIR)

Review after the implementation of a *change* that determines if the *change* was successful

Note: Depending on the specific type and complexity of the *change*, the post implementation review may vary widely in its depth.

6.49 Priority

Relative importance of a target, object or *activity*

Note: Often *incidents*, *service requests*, *problems* and *changes* are given a priority. In the case of *incidents* and *problems*, priority is usually based on the specific impact and urgency of the situation.

6.50 Problem

Underlying cause of one or more *incidents* that requires further investigation to prevent *incidents* from recurring or reduce the negative impact on *services*

6.51 Procedure

Specified set of steps or instructions to be carried out by an individual or group to perform one or more *activities* of a *process*

6.52 Process

Structured set of *activities*, with clearly defined responsibilities, that bring about a specific objective or set of results from a set of defined inputs

Note: Generally, a process consists of a number of *activities* used to manage *services*, if the process is part of a *service management system (SMS)*.

6.53 Record

Documentation of an event or of the results of performing a *process* or *activity*

6.54 Release

Set of one or more *changes* to *configuration items (CIs)* that are grouped together and deployed as a logical unit

6.55 Release and deployment strategy

Approach taken to manage releases and their deployment for a given set of *service components* and related *configuration items (CIs)*, including organisational and technical aspects of planning, building, testing, evaluating, accepting and deploying releases

Note: Typical release and deployment strategies include continuous integration (a DevOps practice where changes to software source code are regularly merged into a central repository, followed by running automated builds and tests) and fixed release cycles (where minor and major releases are planned according to a long-term schedule, with emergency releases being deployed between release cycles as necessary).

6.56 Request for change (RFC)

Documented proposal for a *change* to be made to one or more *configuration items (CIs)*

6.57 Risk

Possible negative occurrence that would have a negative impact on the *service provider's* ability to deliver agreed *services* to *customers*, or that would decrease the *value* generated through some *service*

Note: Risk is made up of the probability of the threat entailed, the vulnerability to that threat of some asset, and the impact the threat would have, if it occurred.

6.58 Role

Set of responsibilities and connected behaviours or actions collected into a logical unit that can be assigned to an individual or group

Note: An individual may take over multiple roles.

6.59 Service

Way to provide *value* to *customers* through bringing about results that they want to achieve

Note: In the context of the FitSM standard series, when referring to services, usually *IT services* are meant.

6.60 Service acceptance criteria (SAC)

Criteria that must be fulfilled by the time a new or changed *service* is deployed and made available to *customers / users*

Note: SAC are defined when a new or changed *service* is designed, and they may be updated or refined during the development or transition phase. They may cover functional and non-functional aspects of the specific *service* to be deployed. SAC are part of the *service design and transition package (SDTP)*.

6.61 Service catalogue

Customer-facing list of all live *services* offered along with relevant information about these *services*

Note: The service catalogue can be regarded as a filtered version of and *customers'* view on the *service portfolio*.

6.62 Service component

Logical part of a *service* that provides a function enabling or enhancing a *service*

Note 1: A *service* is usually composed of several service components.

Note 2: A service component is usually built from one or more *configuration items (CIs)*.

Note 3: Although a service component underlies one or more *services*, it usually does not create *value* for a *customer* alone and is therefore not a *service* by itself.

6.63 Service design and transition

Entirety of steps to be taken to plan and develop a new or changed *service* and to deploy the new or changed *service* to the live environment.

Note 1: Service design and transition plans, sometimes referred to as the service design and transition package (SDTP), should be produced for every new or changed service. It may consist of a number of documented plans and other relevant information, available in different formats, including a list of requirements and *service acceptance criteria (SAC)*, a project plan, communication and training plans, technical plans and specifications, resource plans, development and deployment schedules / timetables, etc.

Note 2: Sometimes, the term transformation is used in situations, when *services* or *service components* are moved from one *service provider* or *supplier* to another.

6.64 Service level agreement (SLA)

Documented agreement between a *customer* and *service provider* that specifies the *service* to be provided and the *service targets* that define how it will be provided

6.65 Service management

Entirety of *activities* performed by a *service provider* to plan, deliver, operate and control *services* offered to *customers*

Note 1: The *activities* carried out in the service management context should be directed by *policies* and structured and organised by *processes* and supporting *procedures*.

Note 2: In the context of the FitSM standard series, when referring to service management, usually *IT service management* is meant.

6.66 Service management plan

Overall plan for implementing and operating a *service management system (SMS)*

6.67 Service management system (SMS)

Overall *management system* that controls and supports management of *services* within an organisation or federation

Note: The SMS can be regarded as the entirety of interconnected *policies*, *processes*, *procedures*, *roles*, agreements, plans, related resources and other elements needed and used by a *service provider* to effectively manage the delivery of *services* to *customers*.

6.68 Service portfolio

Internal list that details all the *services* offered by a *service provider*, including those in preparation, live and discontinued

Note: For each *service*, the service portfolio may include information such as its *value* proposition, target *customer* base, *service* description, relevant technical specifications, cost and price, *risks* to the *service provider*, service level packages offered, etc.

6.69 Service provider

Organisation or *federation* (or part of an organisation or *federation*) that manages and delivers a *service* or *services* to *customers*

6.70 Service report

Report that details the performance of a *service* versus the *service targets* defined in *service level agreements (SLAs)* – often based on *key performance indicators (KPIs)*.

Note: The recipients of (different kinds of) service reports may include *customers* as well other relevant parties, such as internal and external *suppliers*, *federation members*, service owners and the SMS owner.

6.71 Service request

User request for information, advice, access to a *service* or a pre-approved *change*

Note: Service requests are often handled by the same *process* and tools as *incidents.*

6.72 Service review

Periodic evaluation of the quality and performance of a *service* together with the *customer* or under consideration of *customer* feedback, from which opportunities for *improvement* are identified, follow-up actions to increase the *value* of the *service* are determined

6.73 Service target

Reference / target values for a parameter used to measure the performance of a *service*, listed in a *service level agreement (SLA)* related to this *service*

Note: Typical *service targets* might include *availability* or resolution time for *incidents*.

6.74 Supplier

Organisation or party that provides a (supporting) *service* or *service component(s)* to the *service provider*, which the *service provider* needs to provide *services* to their *customers* / *users*

Note 1: A supplier may be internal or external to the organisation of the *service provider*.

Note 2: In a *federation*, the *federation members* are regarded as internal suppliers.

6.75 Top management

Senior management within an organisation who has authority to set *policies* and exercise overall control of the organisation

6.76 Underpinning agreement (UA)

Documented agreement between a *service provider* and an external *supplier* that specifies the underpinning *service(s)* or *service component(s)* to be provided by the *supplier*, together with the related *service targets*

Note 1: A UA can be seen as a *service level agreement (SLA)* with an external *supplier* where the *service provider* is in the *customer* role.

Note 2: A UA may also be referred to as an *underpinning contract (UC)*.

6.77 Underpinning contract (UC)

See: *Underpinning agreement (UA)*

6.78 User

Individual that primarily benefits from and uses a *service*

6.79 Value

Benefit to a *customer* and their *users* delivered by a *service*

Note: Value should be considered as a composition of the utility (fitness for purpose) and warranty (fitness for use, covering sufficient *availability* / *continuity*, *capacity* / performance and *information security*) connected to a *service*.

6.80 Workaround

Means of circumventing or mitigating the symptoms of a *known error* that helps to resolve *incidents* caused by this *known error*, while the underlying root cause is not permanently eliminated

Note 1: Workarounds are often applied in a situation, when the actual root cause of (recurring) *incidents* cannot be resolved due to lack of resources or ability.

Note 2: A workaround may consist of a set of actions to be carried out by either the *service provider* or the *user* of the *service*.

Note 3: A workaround is also referred to as a temporary fix or temporary solution.