



Standards for lightweight
IT service management

Part 1: Requirements

Edition 2016 – Version 2.1



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).
<http://www.fitsm.eu/>





Document control

Document Title	Part 1: Requirements
Document version	2.1
Release date	2016-06-14

Table of Contents

1. Foreword.....	1
2. Introduction	1
3. Scope and applicability	2
4. Terms and definitions	2
5. General requirements for a service management system	3
6. Process-specific requirements	5





1. Foreword

FitSM is a lightweight standards family aimed at facilitating service management in IT service provision, including federated scenarios. The main goal of the FitSM family is to maintain a clear, pragmatic, lightweight and achievable standard that allows for effective IT service management (ITSM).

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 science.

FitSM is designed to be compatible with the International Standard ISO/IEC 20000-1 (requirements for a service management system) and the IT Infrastructure Library (ITIL). Although the FitSM process model, requirements, recommended activities and role model target a lightweight implementation, it can act as a first step to introducing “full” ITSM, i.e. applying ITIL good practices and / or achieving compliance against ISO/IEC 20000-1. The FitSM family is made up of several documents, providing guidance and input on different aspects of ITSM in federated ICT infrastructures:

- FitSM-0: Overview and vocabulary
- FitSM-1: Requirements (this document)
- FitSM-2: Objectives and activities
- FitSM-3: Role model
- FitSM-4: Selected templates and samples (*set of documents under continual development*)
- FitSM-5: Selected implementation 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. Introduction

The requirements stated in this part of the FitSM standards series are aimed at supporting effective, lightweight IT service management (ITSM) processes in an organisation (or part of an organisation) delivering IT services to customers, and harmonizing ITSM across federated computing infrastructures. By this we mean situations where, rather than a service provider having hierarchical conventional agreements with suppliers and customers, services are provided by a looser collaboration of organisations acting as a federation.



3. Scope and applicability

This part of the standard provides:

- 16 general requirements for a service management system, grouped in 7 categories;
- 69 process-specific requirements for a service management system, grouped in 14 categories according to the FitSM process model as described in FitSM-0.

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. It is especially suitable for groups new to service management, or for federated scenarios.

4. Terms and definitions

For the purpose of this standard, the terms and definitions according to FitSM-0: Overview and Vocabulary apply.



5. General requirements for a service management system

GR1 Top Management Commitment & Responsibility

REQUIREMENTS

- GR1.1 Top management of the organisation(s) involved in the delivery of services shall show evidence that they are committed to planning, implementing, operating, monitoring, reviewing, and improving the service management system (SMS) and services. They shall:
 - Assign one individual to be accountable for the overall SMS with sufficient authority to exercise this role
 - Define and communicate goals
 - Define a general service management policy
 - Conduct management reviews at planned intervals
- GR1.2 The service management policy shall include:
 - A commitment to fulfil customer service requirements
 - A commitment to a service-oriented approach
 - A commitment to a process approach
 - A commitment to continual improvement
 - Overall service management goals

GR2 Documentation

REQUIREMENTS

- GR2.1 The overall SMS shall be documented to support effective planning. This documentation shall include:
 - Service management scope statement (see GR3)
 - Service management policy (see GR1)
 - Service management plan and related plans (see GR4)
- GR2.2 Documented definitions of all service management processes (see PR1-PR14) shall be created and maintained. Each of these definitions shall at least cover or reference:
 - Description of the goals of the process
 - Description of the inputs, activities and outputs of the process
 - Description of process-specific roles and responsibilities
 - Description of interfaces to other processes
 - Related process-specific policies as applicable
 - Related process- and activity-specific procedures as required
- GR2.3 The outputs of all service management processes (see PR1-PR14) shall be documented, and the execution of key activities of these processes recorded.
- GR2.4 Documentation shall be controlled, addressing the following activities as applicable:
 - Creation and approval
 - Communication and distribution
 - Review
 - Versioning and change tracking



GR3 Defining The Scope Of Service Management

REQUIREMENTS

- GR3.1 The scope of the SMS shall be defined and a scope statement created.

GR4 Planning Service Management (PLAN)

REQUIREMENTS

- GR4.1 A service management plan shall be created and maintained.
- GR4.2 The service management plan shall at minimum include or reference:
 - Goals and timing of implementing the SMS and the related processes
 - Overall roles and responsibilities
 - Required training and awareness activities
 - Required technology (tools) to support the SMS
- GR4.3 Any plan shall be aligned to other plans and the overall service management plan.

GR5 Implementing Service Management (DO)

REQUIREMENTS

- GR5.1 The service management plan shall be implemented.
- GR5.2 Within the scope of the SMS, the defined service management processes shall be followed in practice, and their application, together with the adherence to related policies and procedures, shall be enforced.

GR6 Monitoring And Reviewing Service Management (CHECK)

REQUIREMENTS

- GR6.1 The effectiveness and performance of the SMS and its service management processes shall be measured and evaluated based on suitable key performance indicators in support of defined or agreed targets.
- GR6.2 Assessments and audits of the SMS shall be conducted to evaluate the level of maturity and compliance.

GR7 Continually Improving Service Management (ACT)

REQUIREMENTS

- GR7.1 Nonconformities and deviations from targets shall be identified and corrective actions shall be taken to prevent them from recurring.
- GR7.2 Improvements shall be planned and implemented according to the Continual Service Improvement Management process (see PR14).



6. Process-specific requirements

PR1 Service Portfolio Management (SPM)

REQUIREMENTS

- PR1.1 A service portfolio shall be maintained. All services shall be specified as part of the service portfolio.
- PR1.2 Design and transition of new or changed services shall be planned.
- PR1.3 Plans for the design and transition of new or changed services shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria.
- PR1.4 The organisational structure supporting the delivery of services shall be identified, including a potential federation structure as well as contact points for all parties involved.

PR2 Service Level Management (SLM)

REQUIREMENTS

- PR2.1 A service catalogue shall be maintained.
- PR2.2 For all services delivered to customers, SLAs shall be in place.
- PR2.3 SLAs shall be reviewed at planned intervals.
- PR2.4 Service performance shall be evaluated against service targets defined in SLAs.
- PR2.5 For supporting services or service components provided by federation members or groups belonging to the same organisation as the service provider or external suppliers, OLAs and UAs shall be agreed.
- PR2.6 OLAs and UAs shall be reviewed at planned intervals.
- PR2.7 Performance of service components shall be evaluated against operational targets defined in OLAs and UAs.

PR3 Service Reporting Management (SRM)

REQUIREMENTS

- PR3.1 Service reports shall be specified and agreed with their recipients.
- PR3.2 The specification of each service report shall include its identity, purpose, audience, frequency, content, format and method of delivery.
- PR3.3 Service reports shall be produced. Service reporting shall include performance against agreed targets, information about significant events and detected nonconformities.



PR4 Service Availability & Continuity Management (SACM)

REQUIREMENTS

- PR4.1 Service availability and continuity requirements shall be identified taking into consideration SLAs.
- PR4.2 Service availability and continuity plans shall be created and maintained.
- PR4.3 Service availability and continuity planning shall consider measures to reduce the probability and impact of identified availability and continuity risks.
- PR4.4 Availability of services and service components shall be monitored.

PR5 Capacity Management (CAPM)

REQUIREMENTS

- PR5.1 Service capacity and performance requirements shall be identified taking into consideration SLAs.
- PR5.2 Capacity plans shall be created and maintained.
- PR5.3 Capacity planning shall consider human, technical and financial resources.
- PR5.4 Performance of services and service components shall be monitored based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.

PR6 Information Security Management (ISM)

REQUIREMENTS

- PR6.1 Information security policies shall be defined.
- PR6.2 Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks.
- PR6.3 Information security policies and controls shall be reviewed at planned intervals.
- PR6.4 Information security events and incidents shall be given an appropriate priority and managed accordingly.
- PR6.5 Access control, including provisioning of access rights, for information-processing systems and services shall be carried out in a consistent manner.



PR7 Customer Relationship Management (CRM)

REQUIREMENTS

- PR7.1 Service customers shall be identified.
- PR7.2 For each customer, there shall be a designated contact responsible for managing the customer relationship and customer satisfaction.
- PR7.3 Communication mechanisms with customers shall be established.
- PR7.4 Service reviews with the customers shall be conducted at planned intervals.
- PR7.5 Service complaints from customers shall be managed.
- PR7.6 Customer satisfaction shall be managed.

PR8 Supplier Relationship Management (SUPPM)

REQUIREMENTS

- PR8.1 Suppliers shall be identified.
- PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with the supplier.
- PR8.3 Communication mechanisms with suppliers shall be established.
- PR8.4 Supplier performance shall be monitored.

PR9 Incident & Service Request Management (ISRM)

REQUIREMENTS

- PR9.1 All incidents and service requests shall be registered, classified and prioritized in a consistent manner.
- PR9.2 Prioritization of incidents and service requests shall take into account service targets from SLAs.
- PR9.3 Escalation of incidents and service requests shall be carried out in a consistent manner.
- PR9.4 Closure of incidents and service requests shall be carried out in a consistent manner.
- PR9.5 Personnel involved in the incident and service request management process shall have access to relevant information including known errors, workarounds, configuration and release information.
- PR9.6 Users shall be kept informed of the progress of incidents and service requests they have reported.
- PR9.7 There shall be a definition of major incidents and a consistent approach to managing them.



PR10 Problem Management (PM)

REQUIREMENTS

- PR10.1 Problems shall be identified and registered based on analysing trends on incidents.
- PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on the services.
- PR10.3 If a problem is not permanently resolved, a known error shall be registered together with actions such as effective workarounds and temporary fixes.
- PR10.4 Up-to-date information on known errors and effective workarounds shall be maintained.

PR11 Configuration Management (CONFM)

REQUIREMENTS

- PR11.1 Configuration item (CI) types and relationship types shall be defined.
- PR11.2 The level of detail of configuration information recorded shall be sufficient to support effective control over CIs.
- PR11.3 Each CI and its relationships with other CIs shall be recorded in a configuration management database (CMDB).
- PR11.4 CIs shall be controlled and changes to CIs tracked in the CMDB.
- PR11.5 The information stored in the CMDB shall be verified at planned intervals.
- PR11.6 Before a new release into a live environment, a configuration baseline of the affected CIs shall be taken.

PR12 Change Management (CHM)

REQUIREMENTS

- PR12.1 All changes shall be registered and classified in a consistent manner.
- PR12.2 All changes shall be assessed and approved in a consistent manner.
- PR12.3 All changes shall be subject to a post implementation review and closed in a consistent manner.
- PR12.4 There shall be a definition of emergency changes and a consistent approach to managing them.
- PR12.5 In making decisions on the acceptance of requests for change, the benefits, risks, potential impact to services and customers and technical feasibility shall be taken into consideration.
- PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes, and proposed deployment dates, which shall be communicated to interested parties.
- PR12.7 For changes of high impact or high risk, the steps required to reverse an unsuccessful change or remedy any negative effects shall be planned and tested.



PR13 Release & Deployment Management (RDM)

REQUIREMENTS

- PR13.1 A release policy shall be defined.
- PR13.2 The deployment of new or changed services and service components to the live environment shall be planned with all relevant parties including affected customers.
- PR13.3 Releases shall be built and tested prior to being deployed.
- PR13.4 Acceptance criteria for each release shall be agreed with the customers and any other relevant parties. Before deployment the release shall be verified against the agreed acceptance criteria and approved.
- PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers.
- PR13.6 Releases shall be evaluated for success or failure.

PR14 Continual Service Improvement Management (CSI)

REQUIREMENTS

- PR14.1 Opportunities for improvement shall be identified and registered.
- PR14.2 Opportunities for improvement shall be evaluated and approved in a consistent manner.