Standards for lightweight IT service management

Part 1: Requirements

Version 3.0.1

Document control

Document title	FitSM-1: Requirements
Document version	3.0.1
Release date	2024-05-21

Contents

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

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 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 other ITSM frameworks such as the International Standard ISO/IEC 20000 and ITIL good practices. 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
- FitSM-1: Requirements (this document)
- FitSM-2: Process activities and implementation
- FitSM-3: Role model
- FitSM-4: Templates and samples *(set of documents under continual development)*
- FitSM-5: 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.

2. About this document

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 federations and multiple providers.

This part of the standard provides:

- 17 general requirements for a service management system (SMS), grouped in 7 categories;
- 65 process-specific requirements for an SMS, grouped in 14 categories according to the FitSM process model as described in FitSM-0.

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

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

3. General requirements for a service management system

GR1 Top Management Commitment & Accountability (MCA)

REQUIREMENTS

- GR1.1 A member of top management of the service provider(s) involved in the delivery of services shall be assigned as the SMS owner to be accountable for the overall SMS.
- GR1.2 A general service management policy shall be defined that includes overall service management goals as well as a commitment to continual improvement and a service-oriented and process-oriented approach. The service management policy shall be approved and communicated to relevant parties by the SMS owner.
- GR1.3 The SMS owner shall conduct management reviews at planned intervals.

GR2 Documentation (DOC)

REQUIREMENTS

- GR2.1 The key elements of the SMS shall be documented to support effective planning. This documentation shall include the SMS scope statement (see GR3), the general service management policy (see GR1) as well as the 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 include:
  - 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 needed
  - Related process- and activity-specific procedures as needed
- GR2.3 The key outputs of all service management processes (see PR1-PR14) shall be documented and the execution of key activities of these processes recorded.
- GR2.4 Documented information shall be controlled, addressing the following activities as applicable:
  - Creation and approval
  - Communication and distribution
  - Review
  - Versioning and change tracking

GR3 Scope & Stakeholders of IT Service Management (SCS)

REQUIREMENTS

- GR3.1 The stakeholders of the IT services and the SMS shall be identified and their needs and expectations analysed. Relevant legal, regulatory and contractual requirements shall be considered.
- GR3.2 The scope of the SMS shall be defined taking into consideration results from the stakeholder analysis.

GR4 Planning IT Service Management (PLAN)

REQUIREMENTS

- GR4.1 A service management plan shall be created and maintained. It shall include:
  - Goals and timing of implementing or improving the SMS and the related processes
  - Roles and responsibilities
  - Training and awareness activities
  - Technology (tools) to support the SMS
- GR4.2 Any process-specific plan shall be aligned to the overall service management plan.

GR5 Implementing IT 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 & Reviewing IT Service Management (CHECK)

REQUIREMENTS

- GR6.1 The effectiveness 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 goals.
- GR6.2 Assessments or audits of the SMS shall be conducted at planned intervals to evaluate the level of maturity and conformity.

GR7 Continually Improving Service Management (ACT)

REQUIREMENTS

- GR7.1 Nonconformities and deviations from goals shall be identified and actions shall be taken to prevent them from recurring.
- GR7.2 The service management policy, service management plan and all service management processes shall be subject to continual improvement. Respective improvements shall be identified, evaluated and implemented according to the Continual Service Improvement Management process (see PR14).

4. 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 Proposals for new or changed services shall be evaluated based on predicted demand, required resources and expected benefits.
- PR1.3 The evolution of services through their lifecycle shall be managed. This shall include the planning of new services and major alterations to existing services. Plans shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria.
- PR1.4 For each service, the internal and external suppliers involved in delivering the service shall be identified, including, as relevant, federation members. Their contact points, roles and responsibilities shall be determined.

PR2 Service Level Management (SLM)

REQUIREMENTS

- PR2.1 A service catalogue shall be maintained.
- PR2.2 For all services delivered to customers, service level agreements (SLAs) shall be in place and reviewed at planned intervals.
- PR2.3 Service performance shall be evaluated against service targets defined in SLAs.
- PR2.4 For supporting services or service components, underpinning agreements (UAs) and operational level agreements (OLAs) shall be agreed as needed and reviewed at planned intervals.
- PR2.5 Performance of supporting services and service components shall be evaluated against targets defined in UAs and OLAs.

PR3 Service Reporting Management (SRM)

REQUIREMENTS

- PR3.1 Required reports shall be identified. Reporting shall cover performance of services and processes against defined targets, significant events and detected nonconformities.
- PR3.2 Reports shall be agreed with their recipients and specified. The specification of each report shall include its identity, purpose, audience, frequency, content, format and method of delivery.
- PR3.3 Reports shall be produced and delivered to their recipients according to specifications.

PR4 Service Availability & Continuity Management (SACM)

REQUIREMENTS

- PR4.1 Service availability and continuity requirements shall be identified and reviewed at planned intervals, taking into consideration SLAs.
- PR4.2 Service availability and continuity risks shall be assessed at planned intervals.
- PR4.3 Appropriate measures shall be taken to reduce the probability and impact of identified availability and continuity risks and meet identified requirements.
- 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 and reviewed at planned intervals, taking into consideration SLAs and predicted demand.
- PR5.2 Current capacity and utilisation shall be identified.
- PR5.3 Future capacity shall be planned to meet identified requirements, considering human, technical and financial resources.
- PR5.4 Performance of services and service components shall be analysed based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.

PR6 Information Security Management (ISM)

REQUIREMENTS

- PR6.1 Information security requirements shall be identified and information security policies defined and reviewed at planned intervals.
- PR6.2 Information security risks shall be assessed at planned intervals.
- PR6.3 Physical, technical and organisational information security controls shall be implemented to reduce the probability and impact of identified information security risks and meet identified requirements.
- PR6.4 Information security events and incidents shall be handled in a consistent manner.
- PR6.5 Access control, including provisioning of access rights, 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 relationship with them.
- PR7.3 Channels used to communicate with each customer, including mechanisms for service ordering, escalation and complaint shall be established.
- PR7.4 Service reviews with customers shall be conducted at planned intervals.
- PR7.5 Service complaints from customers shall be handled in a consistent manner.
- PR7.6 Customer satisfaction shall be managed.

PR8 Supplier Relationship Management (SUPPM)

REQUIREMENTS

- PR8.1 Internal and external suppliers shall be identified.
- PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with them.
- PR8.3 Channels used to communicate with each supplier, including escalation mechanisms, shall be established.
- PR8.4 Suppliers shall be evaluated at planned intervals.

PR9 Incident & Service Request Management (ISRM)

REQUIREMENTS

- PR9.1 All incidents and service requests shall be registered, classified and prioritised in a consistent manner, taking into account service targets from SLAs.
- PR9.2 Incidents shall be resolved and service requests fulfilled, taking into consideration information from SLAs and on known errors, as relevant.
- PR9.3 Functional and hierarchical escalation of incidents and service requests shall be carried out in a consistent manner.
- PR9.4 Customers and users shall be kept informed of the progress of incidents and service requests, as appropriate.
- PR9.5 Closure of incidents and service requests shall be carried out in a consistent manner.
- PR9.6 Major incidents shall be identified based on defined criteria, and handled in a consistent manner.

PR10 Problem Management (PM)

REQUIREMENTS

- PR10.1 Problems shall be identified and registered in a consistent manner, based on analysing patterns and trends in the occurrence of incidents.
- PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on 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 The scope of configuration management shall be defined together with the types of configuration items (CIs) and relationships to be considered.
- PR11.2 The level of detail of configuration information shall be sufficient to support effective control over CIs.
- PR11.3 Information on CIs and their relationships with other CIs shall be maintained 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.

PR12 Change Management (CHM)

REQUIREMENTS

- PR12.1 All changes shall be registered and classified in a consistent manner. Classification shall be based on defined criteria and consider different types of changes, including emergency changes and major changes.
- PR12.2 For each type of change, steps shall be defined for handling them in a consistent manner.
- PR12.3 Changes shall be assessed in a consistent manner, taking into consideration benefits, risks, potential impact, effort and technical feasibility.
- PR12.4 Changes shall be approved in a consistent manner. The required level of approval shall be determined based on defined criteria.
- PR12.5 Changes shall be subject to a post implementation review as needed, and closed in a consistent manner.
- PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes and intended deployment dates, which shall be communicated to interested parties.

PR13 Release & Deployment Management (RDM)

REQUIREMENTS

- PR13.1 Release and deployment strategies shall be defined, together with the service components and CIs to which they are applied. Strategies shall be aligned with the frequency and impact of releases as well as the technology supporting deployment.
- PR13.2 Criteria for including approved changes in a release shall be defined, taking into consideration the applicable release and deployment strategy.
- PR13.3 Deployment of releases shall be planned, including acceptance criteria, as needed.
- PR13.4 Releases shall be built, tested and evaluated against acceptance criteria prior to being deployed. The extent of release testing shall be appropriate to the type of release and its potential impact on services.
- PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment.
- PR13.6 Deployment activities shall be evaluated for success or failure.

PR14 Continual Service Improvement Management (CSI)

REQUIREMENTS

- PR14.1 Opportunities for improvement of services and processes shall be identified and registered, based on reports as well as results from measurements, assessments and audits of the SMS.
- PR14.2 Opportunities for improvement shall be assessed to decide on necessary actions.
- PR14.3 The implementation of actions for improvement shall be controlled in a consistent manner.