D6.1: Service management tools implementation and maturity baseline assessment framework

Deliverable

Document ID	FedSM-D6.1
Status	Final
Version	1.1
Author(s)	Tomasz Szepieniec, All
Due	M10 (31 June 2013)

Abstract

This document introduces the level of tools support assessment framework. The framework is ready for self- or assisted-assessment of FedSM Client as well as any federated provider. The framework is based on the 3 levels of tools support that are independent from capability and maturity levels. Those 3 levels are related both to 14 service management processes and 7 service management general requirements areas. The results should be supportive tool for taking decisions related to tools developments.

Table of Contents

1. Introduction 3
1.1. Contribution to project objectives 3
1.2. Important terms and concepts....4
2. Role of tools in (federated) IT Service Management 4
3. Tools federation challenges 4
3.1. Challenges related to technology seen in federated environments. 5
3.2. Challenges related to ITSM tools....5
4. Assessment framework design methodology 6
4.1. Methodology consideration 6
4.2. Levels definition and scope 7
5. Guidance on the assessment of the level of tool support 9
6. Summary 16
7. References 16

1. Introduction

The FedSM project is built around three key areas on which ITSM is implemented, namely: people, processes and technology. In this document we focus on the last area.

Technology is an important element in ITSM, though it supports and serves rather than drives the process-orientated model seen in most ITSM schemas and frameworks. FedSM does not intend to produce or promote specific tools, but it does seek to assist Federated Infrastructures in supporting their ITSM efforts with appropriate technology.

A lack of appropriate tools may limit value of maturing ITSM or, in some cases, it would not make it possible. This is mainly related with the fact that a proper service management system is about many registered events, linked documents, data, etc., so, the complexity of the system might be quite high. The tools are needed to support parties to deal with the complexity, that would otherwise produce too much manual work overhead. Federated mode of operating services is even more demanding as:

- single data need to be processed and stored by many stakeholders in different locations, and
- different implementations of tools for single process must be interoperable.

The FedSM approach to technology is similar to the way how we are dealing with processes in Work Package 5. The first step, we are focusing in this deliverable, is to understand the role of tools and technologies and then to establish the assessment framework of service assessment tools. The next step is to use this framework for assessing baseline in clients' infrastructure. Based on this assessment it would be possible to identify the most crucial gaps in the tools functionality, that in turn are the basis of plans to improve tool support in the specific processes.

The rest of the document is structured in the following way: first we summarize how this deliverable will contribute to overall FedSM objectives and we introduce new specific terms used in this document. In Section 2 we provide an overview of the role of tools in ITSM, and Section 3 summarizes the challenges that federation brings to implementation of ITSM tools. Having this in mind we describe our approach to assessment framework methodology in Section 4 and finally, we will present the assessment framework itself, in the form of tables, which is ready for self- or assisted-assessment.

1.1. Contribution to project objectives

This deliverable starts with a series of project outputs related to tools. This follows a similar approach as for WP5 and involves:

- Assessing the current state of ITSM tools in client infrastructures using a defined process, looking both at different approaches within and between Federated Infrastructures, but also comparing the status with the tools used in traditional or commercial ITSM (D6.2)
- Identifying the areas where improvement in ITSM tools is necessary, desirable and achievable and prioritizing these changes in collaboration with clients' infrastructures (D6.3)
- Working with client's infrastructures to help them make rational selections in terms of internally or externally sourced ITSM tools to support their more mature service management processes.

1.2.Important terms and concepts

- SMT – Service Management Tools, any software or piece of technology that is used to facilitate operation of one or more ITSM processes.
- Tool - (in context of this deliverable) service management tool (SMT)

2. Role of tools in (federated) IT Service Management

A service management system needs to be adequately supported by tools, on order to function effectively and efficiently.

While the fulfilment of all FitSM requirements [2] and all phases of the PDCA cycle can be facilitated by IT tools, it is the process-specific requirements and the 'Do'-phase, where the support of specialized tools is the most helpful. In the 'Plan' phase often graphical modelling tools are used to create understandable and coherent process definitions. The 'Check'-phase is frequently supported by reporting tools, which help to gather and analyze process-related data. There are tools for generic management disciplines like document control. However, these are all management tasks, which are very similar, whether the provisioning of IT services is managed or other kinds of business. An ITSM-specific tool is usually not needed in these areas.

But in the context of the day-to-day operation of service management processes, well-integrated ITSM-specific tools can provide significant benefits – a fact that is also reflected in the big market for such software in the private sector.

A tool suite for a service management process should be more than just a loose collection of systems and applications, each supporting only individual process activities. For example, email clients and system-monitoring software can be put to good use in the context of incident management, but by themselves they do provide much help in coordinating the process. An optimal solution will enable the communication and coordination of all human actors in the process (an aspect that is especially challenging in a federated ITSM context), but also would enable the correlation of incident data with information from other processes (e.g. services, changes, configuration items) and other sources.

3. Tools federation challenges

FedSM's work addresses federations and other complex communities who must interact with each other to provide computing services. Federation imposes a wide range of challenges, many if not most of which have to do with people and processes. In fact, within the e-Infrastructure community, a common problem has been trying to use technology as a replacement for improved ITSM processes, training and clear staff roles.

Despite this, a subset of the challenges seen in federated service management relate to tools. These come in two general categories:

1. Tools related to federated service provision that do not extend well to ITSM needs.
2. ITSM tools that do not support federation, and are designed for single service providers.

The following sections give some examples of these sorts of challenges.

3.1.Challenges related to technology seen in federated environments.

While there are many complex computing environments in Europe, the ones we are considering in terms of 'federation' tend to be those that were not planned from day one to grow to the scale and complexity they have or are likely to achieve. Instead federated environments tend to come from the connection of pre-existing and heterogeneous groups into larger consortia driven through need or external pressure. For instance different agencies, companies and public sector organizations may come together around a government-backed IT project. In the e-Infrastructure domain many independent academic computing centers connect to one another to create larger combined services to serve their users.

In both these cases the first challenge tends to be connecting up technical services. This leads to design based on the most realistic way to connect existing technical elements and service components and can result in a system that is optimised for technical interoperability rather than management interoperability. It is difficult to impose, for instance, probes from monitoring parameters that will relate to KPIs and SLAs in these environments. Instead it is after the technical components of the consortium have been connected that the 'infrastructure' for service monitoring and management is retrofitted. This means the investment to implement technology to support service management, and the investment needed to build tools on top of these infrastructures is similarly difficult and expensive. The introduction of ITSM is always difficult and can cause resistance, and the additional overhead of retrofitting it after an already-challenging technical integration can make ITSM introduction even more difficult, and make the resulting IT Service Management more expensive and less effective.

Solving these challenges would ideally include building federations from the bottom up, which is unlikely, but at least implies considering ITSM issues at the same time as technical service provision ones. It also suggests the need for openness to some level of overall technical change for all concerns that can be hard to achieve.

3.2.Challenges related to ITSM tools

Other challenges in instituting federated ITSM relate to the difference between traditional non-federated ITSM tools and those needed in a federated environment. The need for FedSM is based on gaps in the way that traditional ITSM operates compared to the situation in federated environments. For instance, federations tend to lack hierarchy and single points of control that ITSM often assumes.

At a simple level, ITSM tools, while generally similar, are often customized to a single organization, whether it is a single data center or data centers across some international company. If the entities in the federation already have ITSM tools, whether simple ticketing systems or complex ITSM suites, they will be customized in different ways for each consortium members so that the connection between them becomes more complex. Even if no ITSM tools are in place, and are being introduced for the whole federation at one time, finding a single configuration that fulfils requirements for all partners will be challenging and time consuming, or the solution will be sufficient for the overall federation but in some ways unsatisfactory for the individual members.

There are also challenges in passing information between members of a federation. This pertains both to what information is available, what should be shared and how the sharing can occur. One example might be configuration information, held in a Configuration Management Database (CMDB). A CMDB should contain data about all Configuration items in the service infrastructure, from technical components like switches and hard drives though key documents such as legal contracts

and SLAs, to staff role descriptions and software licenses. For a single provider this becomes a single, unifying information system for the service provider that is used to track many aspects of ITSM, from managing changes to tracking faults and ensuring that SLAs are met.

In a federated environment, a CMDB is more complex. Each member of the federation will or should have their own CMDB, which holds all information relevant to them. However it is very unlikely that all elements are related to the aspect of their work that is federated. A federation-level CMDB should in theory pull data from member CMDBs, but it may be difficult to ascertain what information is required. A standard ITSM suite may assume that all equipment belonging to a provider should be listed, but a federation member may need to enter information for a data center where only some of the machines inside are used by the federation. General information pertaining to the whole center may be needed, but only partial information on a machine within it. Worse, if the federation member provides cloud resources, whose components must be listed in the CMDB, may vary frequently each day, yet putting all information in the CMDB may be too difficult or not acceptable in terms of the privacy of data about other users of the data center. A federation CMDB needs to be hierarchical, drawing on local federation member CMDBs, and also be flexible in pulling data that is relevant for current SLAs but cope with not having a complete set of information about all possible elements of the service infrastructure.

In this and other ways, current ITSM tool suites have limitations. They are assumed to be the only solution of their type and operate across the whole service provision community. However, even when they are deployed federation wide they are often not be designed to cope with the partial nature of information flow. Even when a single suite is deployed across a federation, customization will either be varied to suit the individual member, or averaged to suit the federation, in both cases meaning that there are difficult clashes. In more likely scenarios, different members use different suites not intended to talk to systems outside those from the same vendor, and there will be technical issues in making them interact.

Solving these issues does not imply revolutionary change of ITSM tooling. Instead it implies a more flexible and open architecture for passing information between members. This could be achieved through standard-based systems or added layers of infrastructure to support the federation functions, but in either case would be an incremental change.

4. Assessment framework design methodology

4.1. Methodology consideration

Carrying out each management process in scope of FedSM, may require the concurrence of appropriate service management tools (SMT). An SMT may range from just a set of documents describing how to deal with the corresponding process to a set of sophisticated software components, which conveniently deployed in a platform, assist the service provider in fulfilling its goals. Any option in between is also possible. On the other hand, the level in which organizations may have adopted SMTs may also vary very much. It might may be a organization that for some determined process don't rely at all on any SMT whereas others may have extensive use of SMTs.

Therefore, determined the we need to differentiate *the level of tools support* in each ITSM process. This might seem similar to capability or maturity levels on which we build our process assessment framework on (see D5.1)[3], however levels of tools support are quite independent from capability.

This means that in general, it is a provider and federator decision of what kind of SMTs are used to support the process and how far automation is needed.

The decision not to link directly level of tool support with the capability model was the most important one, heavily discussed while designing this framework. Finally, the argument for such solution was the following:

- in the capability model, we focus on how a process is effective, whether it is defined, documented and operated in a predictable manner; therefore the efficiency of the exact implementation, understood as manpower needed to operate the process or overhead related to proper operation, is not covered;
- in general scope it is impossible to decide arbitrarily what kind of support is needed for a specific capability level; this needs to be assessed individually for each provider.

On the other hand, it is generally true that capability levels and tool supports are correlated. So usually, higher capability levels require at least some tool support. For example, it is hard to imagine to operate properly incident management in federated environment using general tools like e-mails and spreadsheets. But at the same time, if an organization is operating this process properly using only such general tools there is no reason to rank their capacity to a lower level.

The requirement for the tools assessment framework was that it should be simple, but in the same time, it should provide enough material to support decision on necessary improvements in tools area.

Any decision on changes on the tools area should be taken on by a provider or federator, based on three factors:

- customer friendliness – is the process operated in the way that is satisfactory for customers? Is the response time for steps in the process satisfactory? Is the progress traceable for customers?
- cost effectiveness – what is the cost of operating services in the current way? How much better tools would reduce operating costs? What is the relation between the costs of introducing and operating better tools (including software licence cost, development/customization, integration, training, process adaptation, etc.) and reducedoperation costs (usually mainly personal effort)
- scalability – is the process ready for higher demand? How much increase of demand (planned, seasonal, occasional) would affect efficiency of the process operation?

4.2.Levels definition and scope

Following the above consideration we decided to introduce 3 levels of tool support, based on the type and level of customization in tools. This made the framework suitable for self-assessment and it is orthogonal to service capabilities.

Definition of those three levels of tool support are the following:

- **Level 0: No tools**
  Definition:
  There is no tool support or tool support is limited to basic communication and documentation using common technology including e-mail or simple non-template-based text-processing
  Comments:

The service management tool support of a given process will be ranked with Level 0 in case that it is carried out without the use of any service management tool. This might be a relatively rare case because the existence of a given process, even at its lowest levels of maturity, will be associated to some form of service management tools.

- **Level 1: General tools**
  Definition:
  Tool support for the process and its activities based on generic tools (including common office software packages, databases, collaboration platforms, etc.) which have been aligned to the process to provide some main features supporting the execution of activities, but not integrated, not supporting all features required for full management, and not using a common data warehouse.
  Comment:
  General supporting tools are in place. This level can be interpreted under different points of view. We can think for instance in the usage of general purpose tools to carry out part or the totality of the process. As an example, imagine the use of spreadsheets to perform a log activity in a given process. Also this level may be used to characterize the existence of a set of tools that are not integrated and may require some sort of translation. Note that, this can be the most common level in many processes.
- **Level 2: Specific tools**
  Definition:
  There are specific tools aligned to topics/process in place, supporting all required features and information and are well-integrated with each other, allowing data to pass freely between them.
  Comments:
  Specific tools aligned to topics/processes are in place and are well-integrated with each other. In order to assign this level to a given management process, the tool in use must be specific for the purpose it was designed. In case the tool makes use of different components, every component has to be in a common framework. In general the commercial tools existing today to carry out the most common management processes could achieve this level.

Levels of tools support defined in this way are helpful for the service providers to make a decision to improve the tool support in case it is needed. In case no tools are in use (Level 0) we suggest to consider first some general tools, like special e-mail addresses or wiki. In case this kind of solution has been tried and still more support is needed, specialized or customized solution should be considered.

Nevertheless, the three levels defined above would be of little help if they were just applied to general tool support. In fact, different processes would be organized and operated in a completely different way. Also in the assessment framework we needed better description that is related to the specific process. This kind of process-specific description would be a source of ideas of what kind of tools are needed to support this process.

According to FitSM [2] these are the 14 processes that have to be considered for service management in federated infrastructures:

1. Service Portfolio Management
2. Service Level Management
3. Service Reporting
4. Service Continuity & Availability Management
5. Capacity Management
6. Information Security Management
7. Customer Relationship Management
8. Supplier Relationship Management
9. Incident & Service Request Management
10. Problem Management
11. Configuration Management
12. Change Management
13. Release & Deployment Management
14. Continual Service Improvement Management

In addition to describing level of tools support for the 14 above processes we also apply them to the 7 general management requirements areas as described in D3.1. The reason for this was to include in the scope of tools assessment framework matters that are general, cross-processes.

1. Top Management Responsibility
2. Documentation
3. Defining the scope of service management
4. Planning service management
5. Implementing service management
6. Monitoring and reviewing service management
7. Continually improving service management

As the result of our tools assessment framework we applied 3 levels of tools support to 14 processes (identified of PR1..14) and 7 general requirements area (identified as GR1..7).

5. Guidance on the assessment of the level of tool support

Code	Requirement area	Level	Description
PR1	Service Portfolio Management	L0: No tools	Service portfolios are kept as simple word processing document or spreadsheets, discussed in person and by email and other basic communications systems.
		L1: General tools	Service portfolios are produced based on an agreed upon templates and stored in a set location accessible to all relevant parties.
		L2: Specific tools	Service portfolios are in a predetermined format and held in a location that also houses other key service management documents and configuration items. Elements of the portfolio are cross-linked to other related CIs, for instance linked to relevant SLAs and OLAs.

Code	Requirement area	Level	Description
PR2	Service Level Management	L0: No tools	Service Level Agreements are kept in simple word processing documents or spreadsheets or in wiki. Negotiation process is done by direct communication (like, telephone, e-mail) without possibility of changes tracking.
		L1: General tools	Service Level Agreements are kept in repository of documents that follow agreed templates. The repository are maintained according to some specific rules. Negotiations might be kept by direct communication tools (like, telephone, e-mail), but the negotiations steps are registered and changes in SLAs are traceable.
		L2: Specific tools	Service Level Agreements are kept in specialized repository that enable searching by specific values and can produce notification related to SLAs operations. Negotiations are supported by specialized tool that track all changes and can send notifications on negotiation steps and other events.
PR3	Service Reporting	L0: No tools	No specific tool support for service reporting. Reports are created manually, send manually and there is no consistent repository for future reference.
		L1: General tools	Some tools are available to provide data according to report templates. Generic tools (wikis, spreadsheets) for collecting reports are in place.
		L2: Specific tools	The process of reporting is supported by tools in creation of scheduled reports, sending them, and storing in the repository.
PR4	Service Continuity & Availability Management	L0: No tools	Tools for service availability and continuity management does not exist at all
		L1: General tools	Tools for monitoring service availability and continuity are in place. Postprocessing of raw data can also be supported by means of specific data mining and summarization techniques. Also a risk management system defining mitigation and contingency can be established
		L2: Specific tools	Service availability and continuity management is supported by an integrated management system. Service availability and continuity is tracked. Control points for risks are properly deployed. Both reactive and proactive are adopted in the context of a global service availability and continuity plan

Code	Requirement area	Level	Description
PR5	Capacity Management	L0: No tools	Tools for capacity management do not exists at all
		L1: General tools	Monitoring of workload offered to available resources is in place. Nevertheless the output of such monitoring tools is not integrated in the context of global management system
		L2: Specific tools	Monitored data of resources workload is properly processed and used to trigger the appropriate reporting or change management activity. The monitoring and post processing of data may be integrated also with the service level management system
PR6	Information Security Management	L0: No tools	Planning and tracking of information security controls are not supported by tools. Information security incidents are handled using e-mail and related basic technology.
		L1: General tools	Some tools are in place to support the planning, implementation and review of information security controls, like template-based Wiki pages where the controls are documented and specified. Information security incidents can be tracked using some defined way of recording. There is a risk assessment template which is used to identify information security-related assets, vulnerabilities and threats and derive the level of risk from this information.
		L2: Specific tools	A dedicated information security management tool is used supporting information asset management, risk assessment, planning and reviewing of security controls and tracking of information security incidents, allowing to link security controls and information security incidents to assets and/or risks.
PR7	Customer Relationship Management	L0: No tools	No tools in place to manage customer information.
		L1: General tools	Some tools in place, like template-based Wiki pages with which general information about a customer and the identity of the corresponding customer representative within the service provider organization is documented.
		L2: Specific tools	Integrated system that links customer information to customer representatives, history of communication with the customer, service review records and service complaint records.
PR8	Supplier Relationship Management	L0: No tools	No tools in place to manage supplier information.
		L1: General tools	Some tools in place, like template-based Wiki pages with which general information about a supplier.

Code	Requirement area	Level	Description
		L2: Specific tools	Integrated system that links supplier information history of communication, supplier performance records and supplied CIs, service components and assets.
PR9	Incident & Service Request Management	L0: No tools	No tools in place to record, prioritize, escalate etc. incidents and service requests
		L1: General tools	Some tools in place, like mailing lists to which incidents can be reported, e-mail to describe and forward incidents, an Excel sheet to track incidents
		L2: Specific tools	An integrated trouble ticket system allowing central recording, classification, prioritization etc. of incidents and supporting the escalation of incidents and notification of users/customers aligned with procedures
PR10	Problem Management	L0: No tools	No tools in place to record, prioritize, classify etc. problems
		L1: General tools	Some tools in place, like mailing lists to which problems can be reported, e-mail to describe and forward problems, an Excel sheet to track problems
		L2: Specific tools	An integrated problem tracking system allowing central recording, classification, prioritization etc. of problems, as well as tracking their status and linking them to incidents, changes, releases and CIs where applicable.
PR11	Configuration Management	L0: No tools	No tools in place to document CIs. CI data is kept in a variety of formats and various places.
		L1: General tools	Some tools in place, like Excel sheets, simple databases or Wiki templates to document CIs in a standardized manner together with their attributes as well as some relationships between CIs
		L2: Specific tools	An integrated CMDB, allowing central documentation of CIs with their attributes, status and their relationships to other CIs (including services), problems, incidents, changes, releases. The tool also aids in the documentation of configuration baselines and in conducting configuration audits (by comparing CMDB data with data from other sources, e.g. monitoring tools).
PR12	Change Management	L0: No tools	No tools in place to record, classify, follow-up, decide on, schedule etc., changes
		L1: General tools	Some tools in place, like Excel sheet to document changes, e-mail to plan and follow up changes, Word files to document approved changes

Code	Requirement area	Level	Description
		L2: Specific tools	An integrated change management system allowing central recording, assessment, tracking, etc. of changes and decision support in the evaluation of impact due to potential changes aligned with procedures
PR13	Release & Deployment Management	L0: No tools	No tools in place to plan, build and test new or changed services
		L1: General tools	Some tools are in place, e.g. word files to document new releases, e-mails to verify and agree acceptance criteria of new or changed services, spread sheet to keep record of release dates and result of the deployment of new and changed services
		L2: Specific tools	An integrated release and deployment management system providing support to plan, build, test and reverse new or changed services aligned with procedures. The management system also provides support to monitor and to analyse the success or failure of new releases, and to reverse the change if needed
PR14	Continual Service Improvement Management	L0: No tools	No tools in place to record, prioritize and track status of opportunities for improvement.
		L1: General tools	Some tools in place, like a mailing list to address improvement suggestions to and an Excel sheet to track the status of opportunities for improvement.
		L2: Specific tools	An integrated system allowing recording, prioritizing and tracking the status of opportunities for improvement. The system also links opportunities for improvement to services and changes where applicable.
GR1	Top Management Responsibility	L0: No tools	The service management policy or any parts of it released by top management are communicated and documented using basic technology. Management reviews are conducted without the help of tools.
		L1: General tools	The service management policy is produced using an agreed upon template, and stored in a set location accessible to all relevant parties. For performing and recording the results of management reviews, defined templates and checklists exist.

Code	Requirement area	Level	Description
		L2: Specific tools	The service management policy is stored in a central document management system or collaboration platform, together with other service management-related documents. Management reviews are supported by a tool allowing the recording of all steps and findings, and linking the review with relevant reports and audit results.
GR2	Documentation	L0: No tools	No tools in place to document processes, procedures or any other components of the SMS
		L1: General tools	Some tools in place, like MS Word-based templates, file store, intranet pages
		L2: Specific tools	Dedicated SMS document management system available, like a Sharepoint or Wiki covering all SMS document, allowing version tracking / document control etc.
GR3	Defining the scope of service management	L0: No tools	No tool is used to support the scoping process.
		L1: General tools	A template is available for specifying the scoping statement.
		L2: Specific tools	The definition of the scope of the SMS is supported by a tool allowing to link the scope to services or service components.
GR4	Planning service management	L0: No tools	Plans for implementing and improving service management are communicated and documented using basic technology.
		L1: General tools	The service management plan considering the implementation of service management processes and procedures, provision of resources, roles, interfaces and supporting technology is produced and maintained using one or more agreed templates (e.g., MS Word, Excel). The service management plan might also be regarded as a project plan, and therefore, project management tools might be applied.
		L2: Specific tools	A dedicated service management planning tool is used to produce, maintain and track the implementation status of the service management plan. The plan and its steps are connected to policies and plans for specific processes and procedures. Interfaces are modelled using a graphical editor showing the links between the service management processes.

Code	Requirement area	Level	Description
GR5	Implementing service management	L0: No tools	The implementation of the SMS is mainly coordinated using e-mail and web-conferencing (in addition to physical meetings).
		L1: General tools	Communication and training as part of service management implementation is supported by some planning-related templates to support the production of communication and training plans. The implementation status of the SMS is recorded in a Wiki or similar platform. Overall coordination may also take place using a Wiki.
		L2: Specific tools	Implementation efforts are coordinated using a single dedicated platform recording and tracking all activities and linking these activities to specific communication and training plans.
GR6	Monitoring and reviewing service management	L0: No tools	Key performance indicators (KPIs) are measured and evaluated without the help of analysis tools. Also, there are no tools to support internal audits. Results are reported by e-mail to relevant people.
		L1: General tools	Key performance indicators (KPIs) are defined and recorded using defined templates (e.g. MS Excel). There are templates for audit plans and reports. The results from KPI measurements and internal audits are recorded in a set location accessible to all relevant stakeholders.
		L2: Specific tools	Dedicated tools are used to define and record KPIs allowing trend analysis and supporting results reports. Internal Audits are planned and the results recorded and reported using a special tool supporting management system audits.
GR7	Continually improving service management	L0: No tools	Improvement proposals and agreed improvement activities are tracked and coordinated using e-mail and other basic means of communication.
		L1: General tools	Templates are in place to support the recording of feedback and proposals for improving service management. Status tracking of improvements is done by keeping up-to-date information in some pre-defined format in a Wiki or similar.
		L2: Specific tools	A dedicated tool is used to record feedback and proposals for improvement, track the status of agreed improvement and review the progress and effectiveness of actual improvements. Each improvement is linked to the respective SMS component.

6. Summary

This document introduces the level of tools support assessment framework. The framework is ready for self- or assisted-assessment of FedSM Client as well as any federated provider. The framework is based on the 3 levels of tools support that are independent from capability and maturity levels. Those 3 levels are related both to 14 service management processes and 7 service management general requirements areas. The results should be supportive tool for taking decisions related to tools developments.

7. References

[1] FedSM Deliverable D3.1. Business models for Federated e-Infrastructures

[2] FitSM-1:2013: Standard requirements for lightweight service management in federated IT infrastructures http://fedsm.eu/fitsm

[3] FedSM Deliverable D5.1. Process Implementation and Maturity Baseline Assessment Framework

Version History

Version	Date	Author	Change record
0.1	08.05.2013	T.Schaaf, T.Szepieniec, All	ToC, section assignment
0.2	30.05.2013	T.Schaaf, O.Appleton, J. Rubio-Loyola, J.Serrat, T.Szepieniec	Description of levels (sec. 5)
0.3	19.06.2013	M.Brenner, O.Appleton, M.Radecki, J.Serrat, T.Szepieniec	Contribution to all sections
0.5	21.06.2013	T.Szepieniec	Integration, various improvements, preparation to internal review
1.0	01.07.2013	T.Szepieniec, J. Rubio-Loyola, L.Alves S. Grois	Internal review changes, integration and other minor improvements to prepare final version
1.1	30.09.2013	O. Appleton	Minor formatting updates