

D7.2a

EOSC Service Delivery and Management

The *EOSC Future* project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement number 101017536



Version 1
April 2022

D7.2a / EOSC Service Delivery and Management

Lead by EGI Foundation

Authored by Matthew Viljoen (EGI.eu), Frank Manista (JISC), Debora Testi (CINECA),
Alessandro Paolini (EGI.eu), Joao Pina (LIP), Renato Santana (EGI.eu), Pavel Weber (KIT),
John Shepherdson (CESSDA)

Reviewed by Rudolf Dimper (ESRF) & Athanasia Spiliotopoulou (JNP)

Dissemination level of the document

Public

Abstract

This deliverable is a report of work in implementing the framework to support the delivery of services within the EOSC Future project. It also reports the plans for the creation of Core Participation Agreements to define metrics determining required levels of service delivery and to enable the monitoring and reporting of these metrics.

Version History

Version	Date	Authors	Description
V0.1	15/03/2022	Matthew Viljoen (EGI.eu)	Initiation – Proposed ToC – First draft
V0.2	28/03/2022	Matthew Viljoen (EGI.eu), Frank Manista (JISC), Debora Testi (CINECA), Alessandro Paolini (EGI.eu), Joao Pina (LIP), Renato Santana (EGI.eu), Pavel Weber (KIT), John Shepherdson (CESSDA)	Version ready for review
V0.3	01/04/2022	Matthew Viljoen (EGI.eu)	Final Version for circulation to consortium incorporating review comments
V1.0	06/04/2022	M Viljoen (EGI Foundation), Athanasia Spiliotopoulou (JNP), Ron Dekker (TGB), Mike Chatzopoulos (ATHENA)	Submission to EC by PC (ATHENA)

Copyright Notice



This work by Parties of the *EOSC Future* Consortium is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/). The *EOSC Future* project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement number 101017536.

Table of Contents

Abbreviations	2
1 Executive Summary.....	3
2 Introduction.....	4
2.1 Hosting of SMS - Issue Tracking, Wiki and Information Dissemination.....	4
2.2 Setting up of the SMS within EOSC Future and Related Work.....	4
2.3 Application and Adoption of the SMS	5
2.4 Plans and Next Steps	5
3 The Core Participation Agreement.....	6
4 Service Management Operational Processes	7
4.1 Service Portfolio Management.....	7
4.2 Service Ordering and Customer Relationship Management	8
4.2.1 Service order management	8
4.2.2 Customer Relationship management	9
4.3 Supplier and Federation Member Relationship Management.....	10
4.4 Service Availability and Continuity Management.....	10
4.5 Capacity Management	11
4.6 Configuration Management.....	11
4.7 Incident and Service Request Management.....	13
4.8 Change Management and Release and Deployment Management	15
4.9 Continual Service Improvement	16
5 Conclusion	19
Appendix A – The Core Participation Agreement	20
6 References.....	25

Table of Figures

Figure 4.1: Extract of EOSC-Core Services list.....	7
Figure 4.2: SOMBO interface.....	9
Figure 4.3: Example of order request received by the service provider	9
Figure 4.4: KPIs measures in SOMBO	9
Figure 4.5: General Service Data Model.....	11
Figure 4.6: View of the EOSC-Core services represented in the GOCDB	12
Figure 4.7: Service components from the EOSC Monitoring Service in GOSC	13
Figure 4.8: Attributes of the Exchange Service component from the EOSC Monitoring Service	13
Figure 4.9: EOSC Helpdesk Zammad interface	14
Figure 4.10: Change Management Workflow procedures.....	15
Figure 4.11: Jira workflow for CHM	16
Figure 4.12: Proposed JIRA workflow for SMS SFIs	17
Figure 4.13: Proposed JIRA workflow for SFIs of EOSC Core services	17

Abbreviations

Acronym	Definition
CPA	Core Participation Agreement
CAB	Change Advisory Board
CAPM	Capacity Management
CHM	Change Management
CI	Configuration Item
CMDB	Configuration Management Database
CONFM	Configuration Management
CPA	Core Participation Agreement
CSI	Continual Service Improvement
EOSC	European Open Science Cloud
EPOT	EOSC Portal Onboarding Team
ISM	Information Security Management
ISRM	Incident and Service Request Management
KEDB	Known Error Database
MVE	Minimum Viable EOSC
OLA	Operational level agreement
PM	Problem Management
PMB	Project Management Board
RDM	Release and Deployment Management
RfC	Request for Change
SACM	Service Availability and Continuity Management
SDTP	Service Design and Transition Package
SFI	Suggestions for Improvement
SLM	Service Level Management
SMS	Service Management System
SFRM	Supplier Federation member Relationship Management
SOCRM	Service Ordering and Customer Relationship Management
SPM	Service Portfolio Management
SQA	Software Quality Assurance
SRM	Service Reporting Management
SUPPM	Suppliers Relationship Management
TCB	Technical Coordination Board

1 Executive Summary

Along with the EOSC-Exchange, the EOSC-Core provides the technical backbone of the EOSC Portal. Together with the EOSC Interoperability Framework, all functionalities will be provided to enable the end users to exploit resources and carry out their work. The EOSC-Core and EOSC-Exchange rely on key functionalities identified in the Minimum Viable EOSC (MVE)^[14] which are provided by a number of specific services and service components, and which must be delivered in a reliable way if EOSC is to be a success.

EOSC Future WP7 delivers key services that form the EOSC-Core and EOSC-Exchange. Such services comprise the EOSC Portal "back office" (facilitating access of users to the EOSC-Core) as well as the "front office" (the functionalities consumed by the users themselves). However, as described in this deliverable, there are other services necessary for the success of the project.

Reliability of service delivery requires an efficient management system that defines all aspects of service delivery, including strategy, policy, processes including control of the transition to production of newly developed services as well as operational processes. All these are covered by the EOSC Service Management System (SMS) that underpins service delivery within EOSC as part of the EOSC Future project. Indeed, the SMS is itself part of the MVE.

This deliverable provides an overview of the current status of the implementation of the EOSC SMS within EOSC Future since the beginning of the project and its adoption and plans for the remainder of the project. The Core Participation Agreement (CPA) provides a pivotal role in service delivery of the EOSC-Core. Chapter 3 describes work to establish CPAs, and an initial version of the CPA is provided in Appendix A. Chapter 4 provides an update of all operational processes underpinning service delivery, apart from the Information Security Management. Information Security Management is covered in Deliverable 7.5a "Evaluation of (and recommendation for) EOSC Security", which is currently being prepared.

It should be noted that Section 4.9 (Continual Service Improvement) includes plans for an audit of the SMS against the FitSM standards family^[12], in order to provide an independent source for its effectiveness and as a source of improvement suggestions. Although this work was not included in the initial project description of activities, it was felt that doing this would be beneficial to the project.

2 Introduction

This deliverable builds on from D7.1 “EOSC Service Planning” and which presented the initial gap analysis of what was anticipated to be needed by an SMS at the beginning of the project and the state of EOSC SMS work from previous projects. The remainder of this section outlines the main work and achievements since this point.

2.1 Hosting of SMS - Issue Tracking, Wiki and Information Dissemination

The previous instance of the EOSC SMS, on which the present EOSC SMS is largely based, was developed on a wiki tightly coupled with an issue tracking system, using the commercial products Confluence and Jira. This choice enabled many requirements of an SMS to be met - the controlled versioning of information pages (procedures, policies) as well as the handling of workflows (change requests, suggestions for improvement, etc.) These tools were hosted on an "eosc-hub.eu" domain that had been set up by the EOSC-hub project.

It was quickly recognised that a new instance of Confluence[11] and Jira[10] needed to be set up for EOSC Future, with access to private content controlled within the project, and the content of the SMS migrated from the previous project in order to further develop it. This migration work was non-trivial and, as noted in D7.1, should be avoided in the future by using a domain name that will persist after the lifetime of a particular project. At present the domain for these hosting tools is "eoscfuture.eu" and to avoid a similar migration in the future, it should either be agreed to continue using this domain for the SMS after the EOSC Future project or to properly anticipate and plan for a second migration to a permanent domain. This decision should first be agreed by the PMB/SOB and then proposed and agreed by the EOSC Association.

The setting up of the wiki and issue tracking, although primarily targeted to meet requirements of the SMS, proved to be very useful for multiple non-SMS activities needed in the project itself. For example, the issue tracking is central to the implementation of the Actionable Roadmap to facilitate the reporting of progress to the EC and other stakeholders. The wiki is additionally used for generic dissemination purposes through the setting up of a public and private areas. The public area[11] is freely accessible and has content such as the EOSC Training Catalogue and the EOSC Future Glossary. The private areas, in addition to hosting the SMS, contains generic information for project work packages and deliverables prior to release. All people needing to access the private areas are vetted to ensure they are eligible to access the areas.

The necessity of wiki and issue tracking functionality has been recognised as fundamental, not only to a project running the SMS but to EOSC as a whole. It is for this reason that these functionalities are themselves part of the MVE – see[14] and EOSC Future deliverable D2.5a Inventory of Core Functions and Inclusion Criteria[15].

2.2 Setting up of the SMS within EOSC Future and Related Work

Having completed the migration of the prototypal EOSC SMS from the EOSC-hub project to EOSC Future, the roles of process manager and owner were assigned to all processes in the SMS. Then followed the work of reviewing and updating the existing content in order to make it applicable to the services within EOSC Future, in particular the EOSC-Core services. This initial stage of the work is nearing completion at the time of writing this deliverable.

Related work consists of further developing the onboarding workflow for services and catalogues to the EOSC-Exchange. The onboarding workflow is part of the Service Portfolio Management process within the EOSC SMS. Onboarding procedures have been updated and optimised and this work has been reported in the Deliverable D6.2a. Onboarding and integration of external catalogues is a newer activity that is taking place in the EOSC Onboarding Strategy group which includes representatives from external projects representing the Regional, Thematic and Horizontal EOSC catalogues. Once the workflow, procedures, formal agreements and policies regarding the onboarding and integration of external catalogues is agreed and complete, these will also be incorporated into the EOSC SMS.

Other related work is about establishing and documenting the quality assurance for the software development activities in the project, which is an integral aspect of the EOSC-Core service development. This activity started as a Cross WP Working Group of the Technical Coordination Board (TCB) shortly after the kick-off of the project and constitutes an important part of the Continuous Service Improvement process of the SMS.

An important step of the EOSC SMS happened in November 2021 when the plan for a Core Participation Agreement was presented and approved by the PMB. This Agreement sets out clear expectations for the required levels of service delivery and imposes requirements regarding the monitoring and reporting of service levels.

2.3 Application and Adoption of the SMS

An SMS, however well-defined it may be, does not have any value unless it is used by the people involved in the service development and delivery. This requires training on the processes as well as an appreciation of the benefits of the SMS and knowledge of how to use it. The reason that this has not happened so far is due to the time needed to migrate and initially update content within the SMS, as well as the establishment of the approach of the Core Participation Agreement as described in the previous section. At the time of writing, this is now complete and the delay of this work has not been significantly detrimental to the service delivery, as during its first year the service delivery has continued by the service suppliers using the existing processes and SMSes. However, it has lacked an integrated approach needed to ensure consistency across all EOSC-Core services and a means to ensure quality service delivery.

2.4 Plans and Next Steps

The activity of training suppliers of EOSC-Core services is now starting by means of a series of presentations run by staff from the EOSC SMS, focussing on relevant aspects of the SMS as part of Task 7.4 Service Delivery. These presentations are aimed at introducing all operational processes and their procedures within the SMS, the benefits that they have and guidance on how to use them. In some cases, and to avoid duplication, it may be appropriate to “outsource” some aspects of the SMS to the suppliers themselves, if they are already running SMS processes meeting the requirements of the EOSC SMS.

Successful usage of the SMS is necessary for a number of important aspects of service delivery that are reflected in the CPA, for example:

- definition and establishment of service levels and quality of service;
- monitoring of service levels to deduce whether adequate quality of service is achieved;
- reporting of service levels over defined time periods;
- consistent use of the helpdesk (ISRM) along with the establishment of agreed response times for different types of incidents and service request tickets;
- adoption of security policies.

Details of next steps are provided in the following section on a per-process level. However, here follows a high-level overview at a strategic level.

Along with the finalisation and establishment of the CPAs, monitoring is being implemented and recorded across all EOSC-Core services so that reports may be generated for all stakeholders. These reports will continue until the end of the project. After this time, it is hoped that this approach will continue – this is a decision for the EOSC Association.

Continuous Service Improvement is being implemented for the SMS and funding has been identified to run at least one (preferably two) audits of the SMS over the remainder of the project as part of the CSI. The auditing programme will be run against the FitSM standards family^[12] in order to assess the maturity of the SMS and to provide input for further improvement of the SMS.

3 The Core Participation Agreement

As noted in Section 2.2, we have identified a need to define service delivery expectations and to understand whether these expectations are achieved for EOSC Core services underpinning EOSC. These service expectations specify required levels of service delivery and impose requirements regarding the monitoring and reporting of service levels within the project.

A Core Participation Agreement (CPA) covers the delivery of services from a service supplier to the EOSC catalogue, which is an integral aspect of EOSC's activities in delivering services to "customers" of the EOSC Future project. The CPA is essentially the approach that the project is adopting for Service Level Management, and it allows a common understanding between all the stakeholders participating in the project. It also provides a framework for maintaining services at a required quality level and potentially a means of identifying suitable service providers, e.g. should the service supplier not comply with the accepted standards of delivery and fail to meet obligations specified within the CPA, the service supplier could be removed from the catalogue and another suitable service supplier could be identified.

A template for the CPA is currently being prepared and is planned to be finalised and agreed at the TCB and SOB level. The latest version of the CPA, which remains work in progress, is included in this deliverable as Appendix A. An updated version of this deliverable will be provided towards the end of the project (D7.2b) where the finalised CPA - along with the list of services with a signed CPA and the reports of how they are meeting the agreed service levels, will be included.

4 Service Management Operational Processes

This section presents an overview of the status of all SMS operational processes which are currently in production service delivery (apart from Information Service Management, which is covered in D7.5 “Evaluation of (and recommendation for) EOSC Security” and which is currently being finalised).

4.1 Service Portfolio Management

Fundamental to the EOSC SMS is knowing which services are in scope and covered by the SMS processes. The remit of the SMS, as defined within the Description of Activities (DoA), is to “deliver and maintain a complete Service Management System (SMS) for the EOSC-Core”. Thus, it follows that all services within the EOSC-Core are under the scope of the SMS. The DoA mentions services developed as part of WP4 and WP5 (EOSC Portal Back and Front Office) and the Minimum Viable EOSC defines functionality that needs to be fulfilled. A definitive list of services (and service components) needs to be compiled as part of the SMS. There also need to be an indication of which services should be considered as being of “production quality”¹.

The service list has been created in the EOSC Future wiki private space under T7.4[1] and contains information including the service owner, the service supplier, and operational and security contacts:

Service Type	Service	Service Component	Service/Component Owner	Service/Component Supplier	Operational Contact	Security Contact	Supporters	Status	
								PROD	PREPROD
Core	EOSC AAI		@Christos Kanellopoulos						
		EOSC Core Infrastructure Proxy		GRNET, GEANT, EGI	eosc-core-infra-proxy@lists.geant.org (Temporary)	security@eosc-portal.eu		PROD	
		RCauth Certification Authority	@Tiziana Ferrari @Licia Florio @David Groep @Jens Jensen - STFC UKRI	GRNET, Nikhef, STFC, GEANT	ops-management @ rcauth.eu	abuse @ rcauth.eu		PROD	
		IGTF X509 to SAML bridge		GRNET	fim-tech@igtft.net	fim-security@igtft.net		PROD	
		EOSC AAI Federation		GEANT	@Christos Kanellopoulos (Temporary)	@Christos Kanellopoulos (Temporary)		PREPROD	
		EOSC AAI Fabric Monitoring		GRNET	aai-fabric@eosc.grnet.gr	aai-fabric-security@eosc.grnet.gr		PREPROD	
	EOSC Front-Office		@Roksana Wilk						
		EOSC Portal Website	@Roksana Wilk		Cyfronet	@Agnieszka Pulapa	@Wojciech Ziajka w.ziajka@cyfronet.pl		PROD
		EOSC Catalogue and Marketplace	@Roksana Wilk		Cyfronet	@Agnieszka Pulapa	@Wojciech Ziajka w.ziajka@cyfronet.pl		PROD
		EOSC User Dashboard	@Roksana Wilk		Cyfronet	@Agnieszka Pulapa	@Wojciech Ziajka w.ziajka@cyfronet.pl		PREPROD
	EOSC Open Science Statistics (FO/BO)	@Stefania Martziou		OpenAIRE	@Stefania Martziou	security-team@openaire.eu		PROD	

Figure 4.1: Extract of EOSC-Core Services list

As mentioned above, the aim of the EOSC SMS is to cover EOSC-Core services. However, there are other non EOSC-Core services delivered by the project which are also being relied upon by users and other stakeholders. An example of this is the EOSC Observatory, which is labelled as an EOSC Support service. Since the aim of this service is to be delivered with production quality, it was proposed and agreed that this should also be covered under the scope of the EOSC SMS. It is possible that other services may also be added in the future.

It should be noted that the onboarded services within the EOSC-Exchange are not fully under the scope of the EOSC SMS (apart from some exceptions, for example the applicability of ISM Policies and when they integrate with EOSC-Core services such as the Helpdesk, in which case these services are referred to within ISRM). The EOSC-Exchange services are listed within the EOSC Provider Portal.

¹ The definition of what constitutes “production quality” is provided within EOSC in the EOSC Portal (<https://eosc-portal.eu/providers-documentation/eosc-provider-portal-resource-maturity-classification>) as TRL 8. The application of this to the EOSC-Core services was proposed and agreed within WP2.

It should be noted however, that related procedures for the EOSC-Exchange (adding or onboarding service, validating and decommissioning or suspending them within the registry) is fully covered within the SMS - this was reported as part of D6.1 "Registry of Connection, Integration, Validation and Auditing Processes".

Further work within the SPM is to properly define the transition of pre-production to production of newly developed EOSC-Core services. It is likely that this transition will involve a series of checks, e.g.:

- Is the service under the scope of Change Management?
- Has the service created a Capacity Plan and Service Availability and Continuity Plan?
- Is the service monitored?
- Is the service available for integration with other services? If so, has information been provided about the benefits of integration/dependencies that need to be met for integration and the procedure that needs to be followed for integration?

In order to cover the complete service delivery lifecycle, a procedure needs to be defined for the decommissioning of a service. It is yet to be determined whether Service Design and Transition Packages (SDTPs) are required for all EOSC-Core services. Creation of such SDTPs were attempted as part of EOSC-hub project but this required a lot of effort.

4.2 Service Ordering and Customer Relationship Management

The Service Ordering and Customer Relationship Management (SOCRM) is the process aimed at establishing and maintaining relationships with customers. In particular, it focuses on: acting as the first contact point for services requests (orders) originating from the EOSC Portal and Marketplace; the efficient processing of those orders; and maintaining good relationships with the customers asking questions as part of their orders.

With respect to the SOCRM description provided in D7.1 two procedures have now been decommissioned:

- "Responding to EOSC-hub 'Contact Us' requests": these activities are now being included in the ISRM process and new Helpdesk queue structure; so this procedure is not needed anymore.
- "Provide technical support" was mainly related to provide support to users who would like to integrate services from different providers; this will now be included in the "Service Order management" (see below)

The status and next steps for the operational procedures are reported below.

4.2.1 Service order management

As reported already in D7.1, the order management is a mature procedure which is in daily use by the EOSC Future team. A new team of order shifters has been organised who monitor the order requests coming from the EOSC portal and process them with the SOMBO tool. In short, the procedure consists of:

- Order shifters monitor the incoming orders from the EOSC portal with the SOMBO tool (Figure 4.3);
- The order is checked and, if all information is present, the order is assigned to the specific provider; if some information is missing or the user is posting comments then these will be replied to;
- The provider will receive a notification via email containing all the user and order information; in the same form he/she will be able to accept or reject the order request (Figure 4.3);
- Based on the provider's answer, the order shifter will update the status of the order (to approved or rejected) and the user will also see the new status on the EOSC portal.

Even if the procedure is fully operational, work has been done in the last months to improve the SOMBO interface and functionalities to better support the work of the order shifters. Requirements in this sense have been provided to the developers and a new release is now deployed which includes:

- Improved functionality to remove spam/testing orders;
- Automatic collection of KPIs (Figure 4.4);
- Better grouping of orders within the same project to spot requests for service composition more easily (Figure 4.2).

Epic		Service Order							Order Target		Test	
Id	Summary	Status	Id	Creation	Update	Status	Service	Offer				
EDSCSO-3353		Active	EDSCSO-3354	2022-03-22T18:01	2022-03-23T09:21	In progress	EGI Cloud Compute	Compute intensive	support@egi.eu	Gianlu Dalla Torre	0	0
EDSCSO-3326		Active	EDSCSO-3334	2022-03-11T11:23	2022-03-11T12:06	In progress	ADAM Platform	offer	N.A.	N.A.	0	0
EDSCSO-3383		Active	EDSCSO-3287	2021-12-22T08:31	2021-12-23T09:52	In progress	EGI Cloud Container Co...	High memory	N.A.	Debora Testi	0	0
			EDSCSO-3264	2021-12-23T21:19	2022-01-18T17:05	In progress	EGI Check-In	As bridge to EGI servic...	N.A.	Valeria Andiccone	1	0
EDSCSO-3254		Active	EDSCSO-3289	2021-12-18T08:52	2021-12-23T09:06	In progress	EGI Cloud Compute	GPU	support@egi.eu	Debora Testi	0	0
EDSCSO-2913		Active	EDSCSO-2915	2021-01-21T11:54	2021-11-24T11:53	In progress	EGI Cloud Container Co...	Compute intensive	N.A.	Enri Fernández del Castillo	2	0
			EDSCSO-2914	2021-01-21T11:45	2021-12-23T09:08	In progress	Full notebook	PAN Demo	N.A.	Debora Testi	1	0
EDSCSO-3283		Active	EDSCSO-3284	2021-11-11T18:19	2021-12-23T09:37	In progress	820HARE	For Large datasets	helpdesk@eudat.eu	Debora Testi	1	0
EDSCSO-777		Active	EDSCSO-876	2020-05-11T08:13	2020-04-24T14:30	In progress	Dynamic On Demand An...	EOSAS Portal	N.A.	Debora Testi	1	0
			EDSCSO-848	2020-05-11T08:05	2020-05-24T09:23	In progress	100 Percent EE Enabled C...	Offer	N.A.	Stefano Le Rocca	2	0

Figure 4.2: SOMBO interface

Request	Value
Amount of RAM	4
Number of cores	1
Persistent storage	1

Resource center	Contact	Resources Cloud	Start	End	Ava	Rel	Action
100IT	N.A	Amount of RAM : 4 Number of cores : 1 Persistent storage : 1	24/03/2022	24/03/2023	90%	95%	<div style="display: flex; gap: 10px;"> <div style="background-color: #28a745; color: white; padding: 5px; border-radius: 5px;">Validate the resource request</div> <div style="background-color: #dc3545; color: white; padding: 5px; border-radius: 5px;">Reject the resource request</div> </div>

Figure 4.3: Example of order request received by the service provider

Month	SOCRM.1	SOCRM.2	SOCRM.3	SOCRM.4	SOCRM.5	SOCRM.6
2022-03	89.63%	71.87%	25.98%	5.53 d	21	0.68 d
2022-02	89.6%	71.89%	26.91%	5.72 d	19	0.11 d
2022-01	89.26%	70.55%	27.81%	5.91 d	8	0.5 d
2021-12	89.28%	70.71%	27.85%	5.99 d	21	0.18 d
2021-11	89.61%	70.31%	28.75%	6.21 d	23	2.44 d
2021-10	89.53%	70.34%	29.06%	6.38 d	11	1.84 d
2021-09	89.3%	69.7%	28.91%	6.48 d	9	1.81 d
2021-08	89.11%	69.15%	29.43%	6.57 d	7	0 d
2021-07	88.95%	68.91%	29.65%	6.66 d	19	0.78 d
2021-06	88.51%	67.87%	30.42%	6.9 d	7	7.84 d

Figure 4.4: KPIs measures in SOMBO

In the next period, it would be useful to explore if it is possible to include a mechanism for the service providers to provide updates on the status of an order. At present, when an order is assigned to the provider, the provider can accept or reject the request (Figure 4.3), but after this step, the order management team would receive no further updates whether the user's request has been satisfactorily served.

Updates to the procedure are also needed to better clarify the process in case of a service request from multiple providers and thus some level of service integration. Even if not many requests of this type are being received at the moment, we believe it would be important to have this step documented in the procedure. This step of the procedure will consist in identifying the multiple provider request in SOMBO and make the providers aware that possibly requirements in terms of integration is foreseen as part of the order they are receiving.

4.2.2 Customer Relationship management

On the customer management side, the part related to maintaining contact with customers making orders is stable and operational and no major changes are foreseen. For customer satisfaction, while the basic principles of collecting users' feedback are in place, actual surveys have not yet been realised. After internal discussion, it

is considered that these surveys might be important for the EOS-Core services more than for the EOSC-Exchange. The target of the surveys might then be the service providers which have integrated one or more of the EOSC-Core services. Further analysis will be carried out to better scope the potential survey.

4.3 Supplier and Federation Member Relationship Management

Suppliers Relationship Management (SUPPM) ensures that a healthy relationship with the suppliers is maintained and that they are supported in delivering services to customers. The suppliers are registered in a database with associated contacts, services delivered, and related agreements. The suppliers' performance is periodically monitored according to the conditions defined in the agreement for the provision of the service the given supplier is involved in.

In the context of EOSC Future, we have registered in the database all of the suppliers delivering the EOSC -Core Services, for which the Core Participation Agreement is going to be negotiated. Besides maintaining the suppliers' database, a procedure was also defined to produce a suppliers' performance report, in coordination with the SACM process: any violations to the service level targets agreed in the CPA are notified to the suppliers, who are expected to provide justifications and plans for improvements.

Once the CPAs are established, performance reports will be created detailing the above information for 10-monthly reporting periods aligned with the EOSC Future project duration.

4.4 Service Availability and Continuity Management

The purpose of Service Availability and Continuity Management (SACM) is to ensure that the level of service availability delivered by a service meets the service levels targets agreed on in the Operational level agreement (OLA) and the availability needs in general, and that an adequate level of service continuity is guaranteed in case of exceptional events.

The process covers the availability and the reliability of a service and its components, which is done by monitoring in order to promptly intervene when an incident occurs. Performance reports are produced periodically in collaboration with the Supplier Federation member Relationship Management (SFRM) process to provide analysis of problems that have happened and to help proposing plans and solutions for improving the availability of services.

At the same time this process covers regular risk assessment and management exercises to reduce risks of failure or downtime to agreed acceptable levels and to plan and prepare for their recovery. The result of these activities is the creation of a Service Availability and Continuity Plan where a number of risks affecting the availability and continuity of the service is identified and assessed: each risk is rated in terms of likelihood and impact with the definition of countermeasures to implement that should avoid the occurrence of the given risk. Any remaining vulnerability is identified as well, and in case the rating of a risk is considered to be too high in relation to the risk acceptance criteria, a plan to either improve the existing countermeasures or to implement new ones is created, with the aim to either reduce the likelihood of a risk or to mitigate the impact in case a risk occurs.

The plan is completed by a continuity and recovery test, where the continuity of the service and its recovery capacity are tested against a simulated disruption scenario: the performance of this test is useful to spot any issue in the recovery procedures of the service. The plan is then reviewed on a yearly basis.

Concerning the implementation of this process in the EOSC Future context, all the EOSC-Core Services are going to have an associated Availability and Continuity plan. Besides a procedure to create, review, and update such a plan, we have also created a procedure to deal with a major loss of service: in such a situation, it is important to determine if the incident can be dealt with and resolved according to the Availability and Continuity plan, or whether further actions should be undertaken, including an update of the Availability and Continuity plan after the service is restored.

These plans are currently being compiled and we intend to have them all in place before the next update of this deliverable.

4.5 Capacity Management

Capacity Management (CAPM) considers all resources required to deliver the IT service, and plans for short-, medium-, and long-term business, capacity, and performance requirements. In fact, the goal of this process is to ensure that sufficient capacities are provided to meet agreed service levels and performance requirements for services that are part of the catalogue.

One of the key activities of the CAPM is to produce a plan that documents the current level of resource utilisation and service performance and, after consideration of the service strategy and plans to forecast the future requirements for new IT resources, to support the IT services that underpin the business activities.

Indeed, for the capacity plan is important to assess if the capacity of the service is sufficient to respond to current and future demands for the service. Capacity aspects of the service delivery are analysed (human, technical, and financial) with the definition of quantitative parameters to measure the usage and the load of the service. The plan clearly specifies any assumptions made as well as any recommendations quantified in terms of resources required, cost, benefits, impact, etc.: the approach to adjust the capacity of the service in relation to a change in the demand is defined and recommendations on capacity requirements for the next reporting period are provided as well (the capacity plan is reviewed at least twice per year).

The defined procedures within the CAPM process describe the process of creating, updating, reviewing, and approving a capacity plan. As with SACM plans, plans for all EOSC-Core Services are being compiled.

4.6 Configuration Management

Configuration Management (CONFM) is the process that ensures the correct implementation of all policies, procedures and management tools necessary to monitor and implement many of the EOSC Future management processes, like the Change Management (CHM), Problem Management (PM), Incident and Service Request Management (ISRM), as well as the Service Availability and Capacity Management (SACM). The CONFM is a pillar for the whole SMS and in order to implement and run this process, it is necessary to keep the services logical model together with the relationships and dependencies for all parts involved. The EOSC-Core services topology model used for the current implementation was defined during the EOSC-hub project [13] and a generic service implementation can be shown in Figure 4.5.

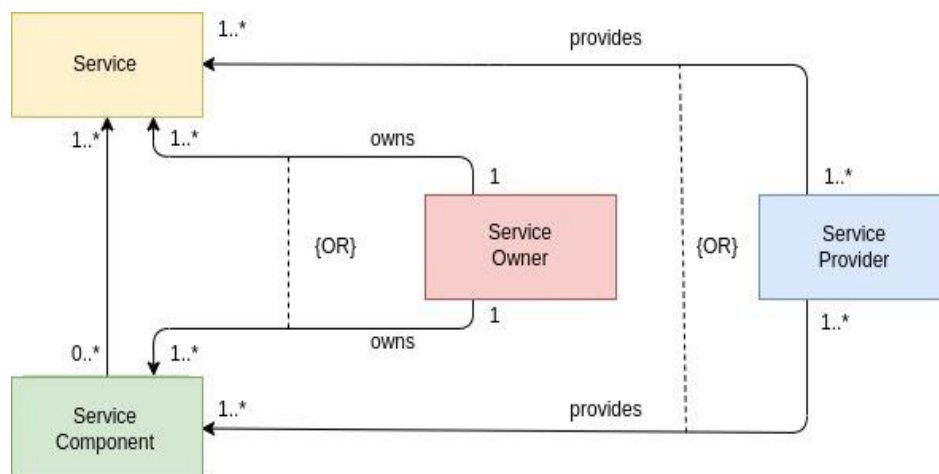


Figure 4.5: General Service Data Model

The arrows and multiplicities between the Component Items (CIs) show possible relationships of the corresponding CIs.

In order to properly implement this model, it is required that all services and their associated information are properly stored. To store this information, an initial schema of a distributed Configuration Management Database (CMDB) was made. The implementation followed a “top-down” schema, meaning that it started by

the creation of a very simplified version of the data model based on the minimum information collected from the core services.

The planned Configuration Items (CI) are the following:

- Service (the single entity formed by a single service component or multiple service components);
- Service provider (legal entity providing the service);
- Service Owner (name/entity of the service Owner);
- Service Components (a single entity with several properties);
 - Service types (a unique identifier, unique name, that is used to distinguish a specific service of type X and Technology Y offered by a provider).
 - Downtimes (severity, classification; starting, ending, declaration and announcement dates; description and affected services) can be declared for one or more services and/or service components;
 - Roles (rules that allow people to perform specific tasks).

This process has already started, it is being implemented using a dedicated EOSC implementation of the GOCD[3] and complemented with the information provided by the CONFM EOSC Future confluence wiki pages[4]. Together with this, a series of procedures was created in order to define how the information should be handled. Figure 4.6 to Figure 4.8 show the services and service components are shown in the GOCD but in order to correlate the services with the different layers used in GOCD the following mapping needs to be made:

```

1st level--> Service == NGI ( GOC_DB_NAME )
2nd level---> Service Component == SITE ( GOC_DB_NAME )
3rd level ---> Service endpoints. == SERVICE ( GOC_DB_NAME )

```

This mapping is required due to the fact that the GOCD uses the same database developed previously for other projects and it is planned to continue developing and adapting it to the EOSC ecosystem.

In the next figures (Figure 4.6 and Figure 4.8) the current EOSC Services and services components implemented in the GOCD are shown.

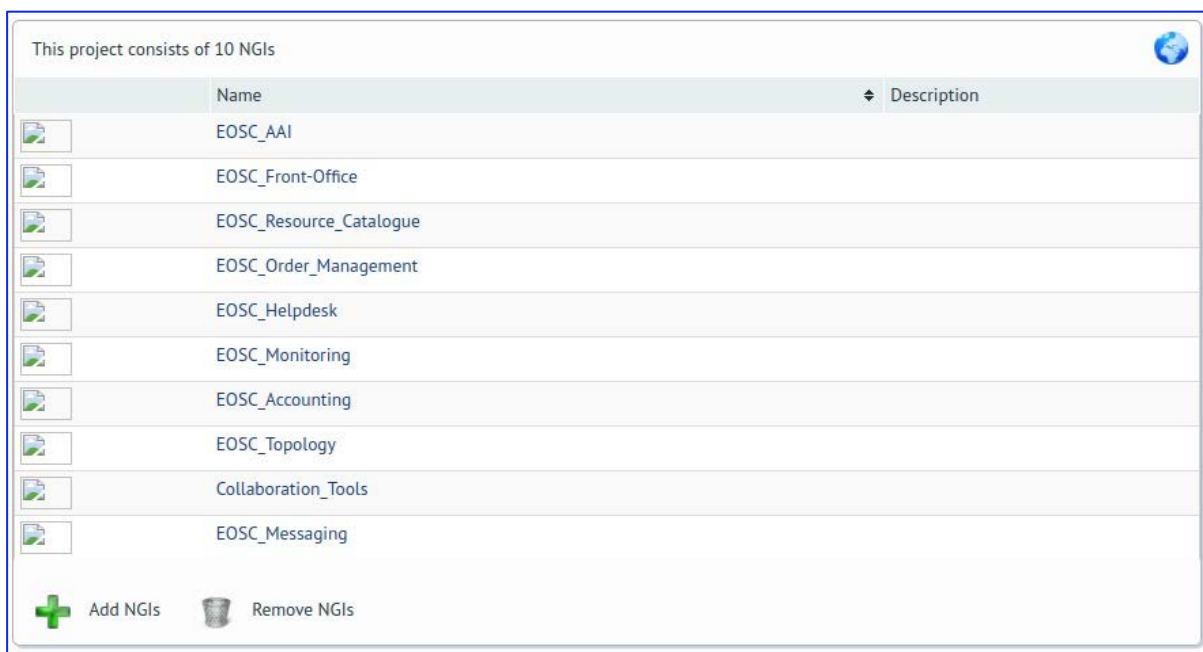


Figure 4.6: View of the EOSC-Core services represented in the GOCD

2 Sites (Note, Scope values marked with (x) indicate the parent NGI does not share that scope)

Name	Certification Status	Production Status	Scope(s)
EOSC_Monitoring_Exchange_Services	Certified	Production	EOSCCore, Local
EOSC_Monitoring_Core_Services	Certified	Production	EOSCCore, Local

Figure 4.7: Service components from the EOSC Monitoring Service in GOSC

The EOSC Monitoring service is composed of two service components for Exchange and Core services.

Site: EOSC_Monitoring_Exchange_Services

EOSC Monitoring for Exchange Services (BO)
EOSC Monitoring for Exchange Services (BO)

Contact Info

E-Mail: argo-ggus-support@grnet.gr

Telephone: +302107474274


Emergency Tel:

CSIRT Tel:

CSIRT E-Mail: argo-ggus-support@grnet.gr

Emergency E-Mail:

Helpdesk E-Mail:

Notifications: 

Project Data

NGI/ROC: EOSC_Monitoring

Infrastructure: Production

Certification Status: Certified Change

Scope Tags: EOSCCore, Local

Networking

Home URL:

GIIS URL:

IP Range:

IP v6 Range:

Domain: argo.grnet.gr

Location

Country: Greece

Latitude:

Longitude:

Time Zone: Europe/Athens

Location:

Figure 4.8: Attributes of the Exchange Service component from the EOSC Monitoring Service

It is foreseen that after the core management processes and procedures are put into place for all the EOSC-Core services the implementation will be analysed and depending on the results a decision process will be established in order to answer the question for which services information data sources should be included in the centralised CMDB and which should be maintained according to the federation scenario. We assume this hybrid approach is a reasonable one and will fit very well to the EOSC ecosystem. During this evaluation, it will also be taken into consideration how EOSC-Exchange Services can be depicted and how their interaction will be done with the EOSC-Core services.

4.7 Incident and Service Request Management

The Incident and Service Request Management (ISRM) process formalises the approach to restore normal / agreed service operation, on the occurrence of an incident and also to receive and deliver the request of a new service. It guarantees the information provided by the users to the ISRM system arrives to the proper support

team. If not properly solved by the first level support (L1 On-Duty), the ticket is assigned to the proper Support Group, for the resolution of incidents, as per procedures defined within the ISRM process[5].

The new service Zammad based EOSC Helpdesk, has been prepared accordingly with the EOSC Future necessities and is under a production and adaptation development state. Therefore, there are still some adaptations needed as more services and users require improvements.

There is a Level 1 rota[6] established and in production, consisting of a general-knowledge group of dedicated personnel, assigned in a “rotation per week” mode, in order to receive and treat tickets concerning incidents and services requests.

There are several ways users can submit a ticket to the support teams regarding an incident, a request for assistance or a new service. This can be done either by sending a simple email, using the EOSC web-portal or via the EOSC Helpdesk Portal. There is more information concerning the way of notifying incidents and requesting assistance or services, as well as a description of the First Level support (L1) and the Group Support at the Helpdesk Guidelines[7].

An example of the EOSC Helpdesk Zammad interface is presented in Figure 4.9:

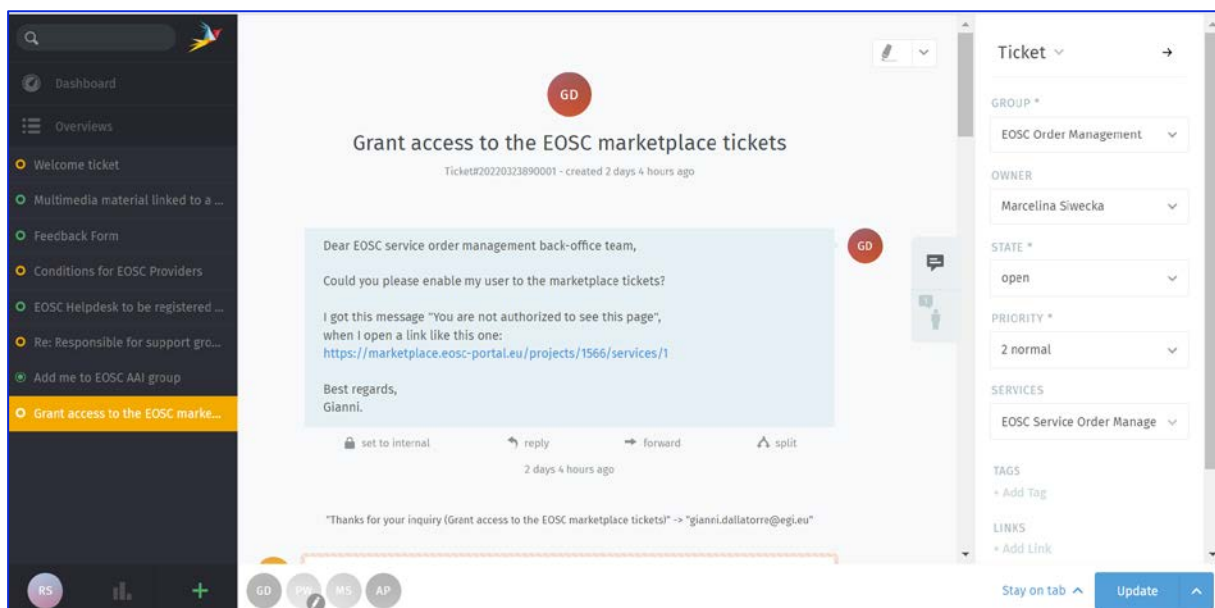


Figure 4.9: EOSC Helpdesk Zammad interface

The main procedures for the EOSC Future helpdesk are related to the way tickets are received and treated. The main goal is to record, classify, prioritise, escalate, resolve and close incidents and services request tickets.

The first level support (L1) has to complete the ticket with all pertinent information. In the case of missing information, the L1 On-Duty has to complete the ticket with the user/client extra info, asking for it. For instance, some ways for a user/client to send a ticket does not make it possible to set the ticket priority. In this case the L1 On-Duty has to provide this information.

After the ticket has complete information, it is possible for the L1 On-Duty to resolve or assign the ticket to the proper Support Group. Having the ticket solved, or not, the proper closing status has to be set either by the L1 On-Duty or by the Support Group. There is more information related to this procedure within the ISRM1 procedure[8].

There are cases where tickets are considered “major incidents” and have a special way to be treated. Major services incidents or degradations need a special procedure[9] to efficiently coordinate the actions between users and the ISRM team, responsible to maintain the service.

4.8 Change Management and Release and Deployment Management

The main task of the EOSC Future Change Management (CHM) is to ensure that changes to the Services Configuration Items (CIs) are planned, approved, implemented and reviewed in a controlled manner avoiding adverse effects to services or customers. Additionally, it provides rules on how to handle Releases, so that these new changes can be tested and deployed to the live environment together. It also oversees (approves, reviews, etc) their implementation in the same manner as single changes.

The Change Management process is a complex process and for easier overview is distributed over four areas: the Change Management Policies, the Types of Changes, the Change Advisory Board (CAB) and process monitoring dashboards (still under preparation).

The procedures describe the workflows for the different types of changes and are built in a modular way, addressing particular issues inside these workflows, like for example the classification of changes or the risk assessment (see diagram below). The procedures state the workflows in the form of actions of the involved entities and their roles. All steps of action are implemented in a dedicated project setup for CHM within the EOSC Future Jira instance[10].

Título	Statement	Procedure status	Procedure owner	Approval status	Next procedure review
CHM1 Open a Request for Change	This procedure describes how to create a Request for Change via opening a JIRA ticket.	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM2 Define a Standard Change	This procedure describes the actions to be taken to put a change on the List of Standard Changes	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM3 Manage Emergency Changes	This procedure describes the workflow for Emergency Changes	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM4 Calculate the Risk Level of a Change	This procedure describes how to evaluate the risk level for a planned change	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM5 Classify a change as Standard or Non-Standard	This procedure describes how to classify a Change Request as Standard or Non-standard Change	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM6 Manage Standard Changes	This procedure describes the workflow for Standard Changes	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM7 Evaluate the risk level for Non-Standard Changes	This procedure describes how to evaluate the risk level of non-standard changes and classify them as normal or high-risk.	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM8 Manage Normal Changes	This procedure describes the workflow for Normal Changes	FINALISED	@ Joao Pina	APPROVED	together with process review
CHM9 Manage High-risk Changes	This procedure describes the workflow for High-Risk Changes	FINALISED	@ Joao Pina	APPROVED	together with process review

Figure 4.10: Change Management Workflow procedures.

The types of changes introduced are three: Standard, Non-Standard and Emergency Changes, where the Non-Standard Changes are further refined into Normal and High-Risk Changes. The three types of changes differ by their risk levels, approval and review steps, and involved entities. The classification of changes into different types allows a more flexible and easy CHM process. The Emergency Changes are exceptional changes, where an immediate reaction is mandatory without being stopped or delayed by a CHM approval. The Standard Changes provide the opportunity to put recurring changes, like for example installation of patches and operating system updates, and service providers have the freedom of reporting or non-reporting this type of changes. The Non-Standard Changes are split into Normal and High-risk according to the EOSC Risk assessment page. Normal and low-risk changes can be handled by service providers whereas high-risk changes need the approval of the Change Advisory Board. The following diagram depicts the current implementation in JIRA of the full CHM process:

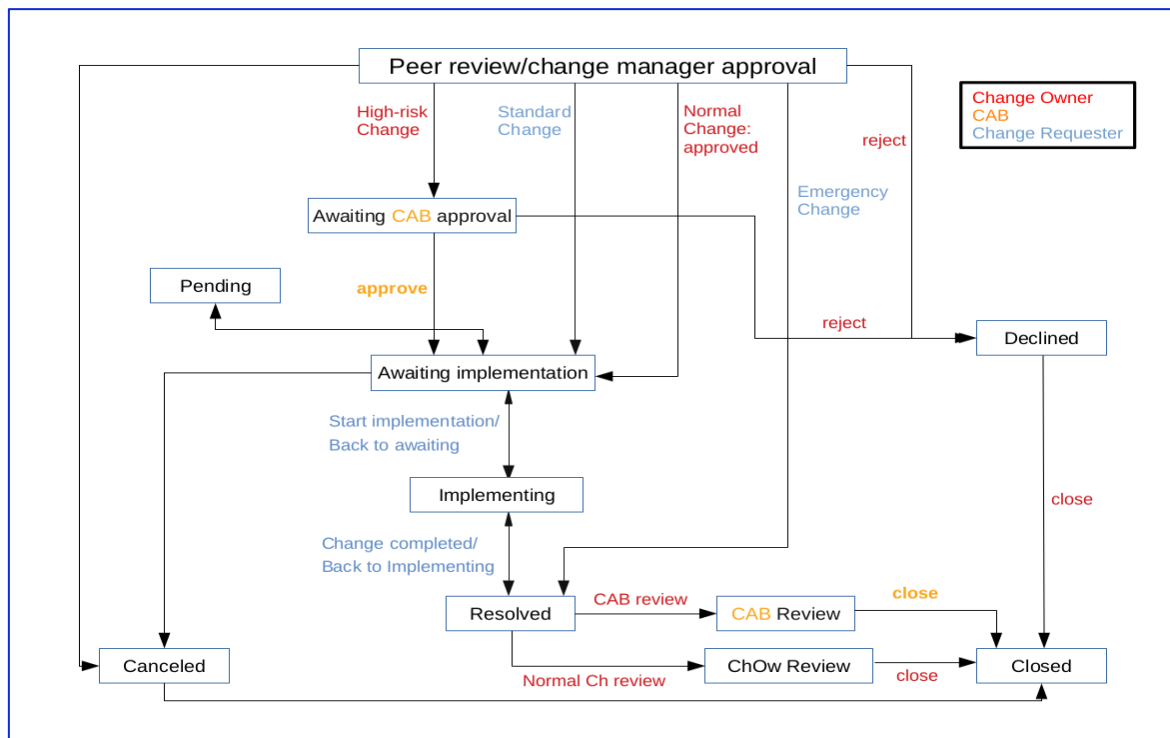


Figure 4.11: Jira workflow for CHM

A JIRA ticket is filled and submitted by the Change Requester, then a staff member of the CHM process will take care of the ticket and steps to be performed by the CHM. The different workflows for the different types of changes involve different statuses and people. The colour of the text attached to the status transitions indicates the person responsible for the corresponding action (Change Request/Implementer, Change Owner or CAB):

In a federation environment like the EOSC, in which some services are composed of multiple Service Components each one with different providers and Owners, some service providers developed their internal Change Management process, like for example the EOSC AAI. Therefore, in those cases, service providers will only be obliged to report High-Risk changes, or changes that directly affect other EOSC-Core services (e.g. a change to an API).

Due to some complexity of the process, and with the need not to burden Service providers and Owners with too many procedures and policies a “how-to” page was created in order to help them to fill the Request for Changes. Also, it’s foreseen to have a dedicated tutorial with service providers on how to interact with the change management process and what are the benefits of having a running change management system.

4.9 Continual Service Improvement

Preparation of the Continual Service Improvement (CSI) process is in hand, and the first version is expected to be ready for use shortly after the submission of this deliverable. Two planning and review meetings have been held with the SMS Manager and a FitSM expert, to determine the scope and approach of CSI, with respect to the needs of the EOSC Future project. It was recognised that as well as providing a means to manage improvements to the SMS, manage the arrangements for internal audits and follow up on their findings, the CSI process should also maintain an overview on any suggestions for improvement for the core services and provide guidance to service developers in respect of Software Quality Assurance (SQA) matters.

The process that will be used to identify, prioritise, plan, implement and review suggestions for improvement (SFIs) to the SMS is extensively elaborated, covering policies, procedures, reports, management reviews, SMS KPIs, SMS process reviews, and a mechanism to gather, prioritise and track progress against suggestions for improvement. The latter are held in a Jira project within the EOSC Jira instance[10], which is monitored and managed as part of the CSI process.

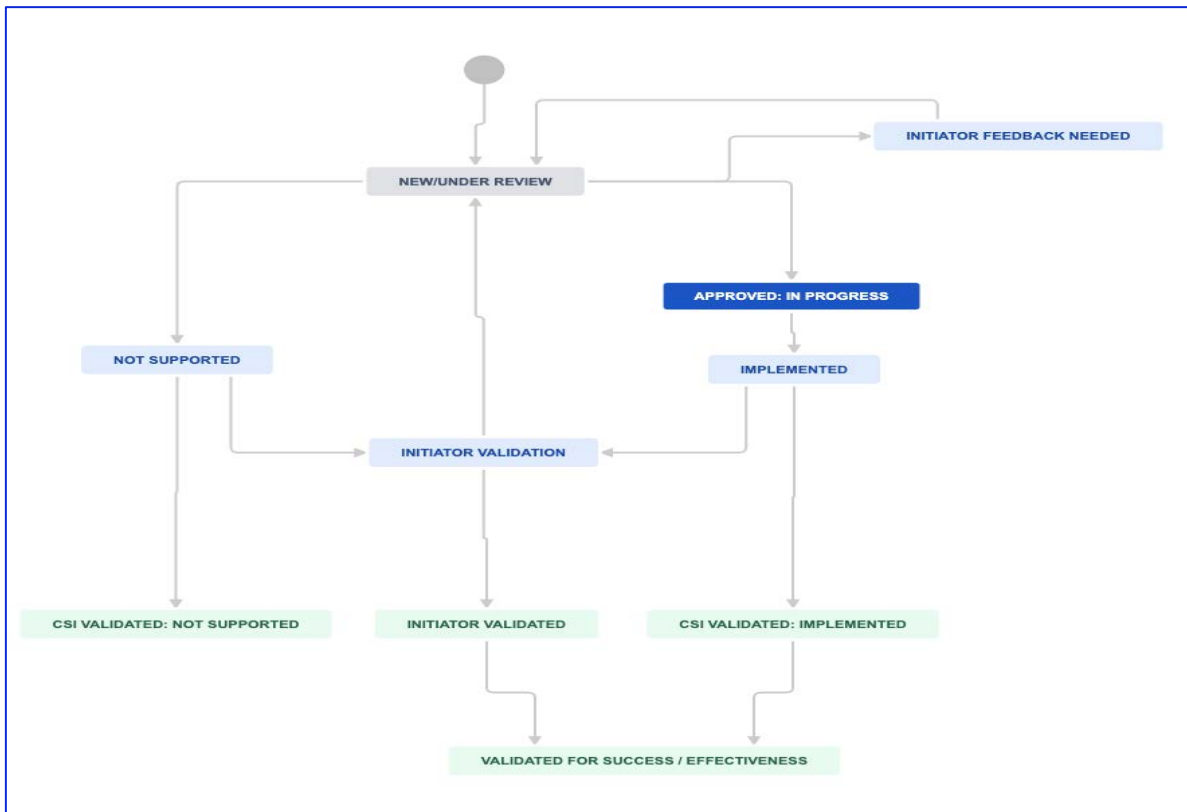


Figure 4.12: Proposed JIRA workflow for SMS SFIs

The internal audit programme will engage the services of auditors who are experts in the FitSM standards family to conduct thorough, comprehensive and well-structured examinations of the efficacy of the SMS. The audit finding will be reported to the appropriate governance bodies of the EOSC Future project and used to drive improvements to the SMS, which in turn will contribute to the quality of the project outcomes.

The suggestions for improvement for the EOSC-Core services are captured via a variety of mechanisms, but are held in a JIRA project, where they are clarified, evaluated and prioritised before being passed to the relevant service engineering team. The CSI process provides oversight, monitoring and reporting on the operation of the relevant JIRA queue, but has no responsibility for determining which, if any SFIs are implemented, or when.

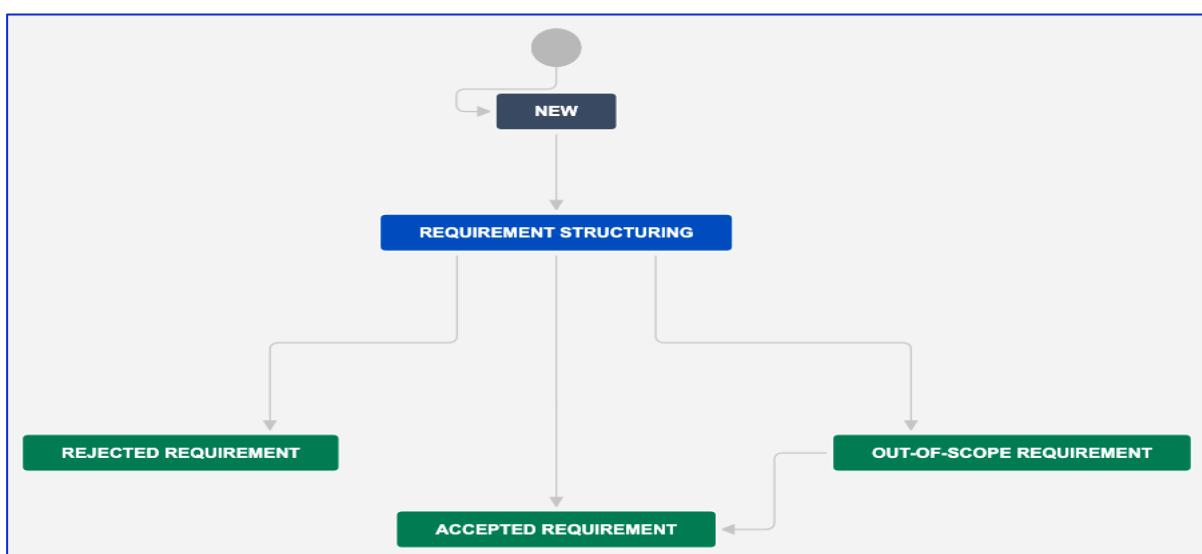


Figure 4.13: Proposed JIRA workflow for SFIs of EOSC Core services

Guidance to service developers in respect of Software Quality Assurance (SQA) matters is provided by a set of guidelines and commentaries, held in the EOSC Future private Wiki space. The guidelines follow on from a survey of EOSC-Core service developers (conducted in the early stages of the project) designed to elicit the current knowledge and implementation of SQA in that community, and any areas where further information was required. The guidelines deal with what should be done, and the commentaries give practical guidance on how to do it, complete with recommendations of tools and utilities to use.

5 Conclusion

This deliverable has aimed to provide a comprehensive update as to the status and readiness of the EOSC SMS to support production service delivery, and to provide an overview of the aspects of service delivery that are being managed by the SMS.

During the first year of the project there was a lengthy process of migration of the SMS from the previous project, which delayed its proper usage. This was described in Section 2.1, along with suggestions of how to avoid such problems in the future. Despite this delay, the EOSC SMS is now fully operational and plans for training the service suppliers on aspects of the SMS that require their input are being established. The SMS is enabling the means to quantify and measure expected levels of service via the Core Participation Agreements, explained in Section 3 which will soon be finalised and signed for the EOSC-Core services.

Appendix A – The Core Participation Agreement

At the time of writing this deliverable, the CPA is still a work in progress and has yet to be presented to and formally approved by the TCB and the SOB. However, it is felt that it is useful to include the latest version of it to provide an indication regarding its likely content.

1. The EOSC Core agreement

PLEASE DO NOT SHARE OUTSIDE EOSC Future project

Status	Draft
Agreement between	EOSC Future and Core Service supplier

2. Document log

Date	Comment	Author

The present The EOSC Core Participation Agreement ('the Agreement') is made between **EOSC Future** and **Core Service supplier** to define the provision and support of the provided service components as described hereafter.

3. The Service component

This agreement covers the delivery of the service(s) described as follows:

Technical	Description of the service/service component

The supplier agrees to fulfil the following obligations:

Coordination	<p>How the supplier should interact with EOSC Future (example):</p> <ul style="list-style-type: none"> • This activity is responsible for the coordination of the service maintenance activities with EOSC T7.4 team and other technology providers for the EOSC Core services • This activity is responsible for the coordination of the system operation and upgrade activities with those partners that are in charge of operating other systems that depend on it
Operational	<p>The internal supplier is responsible for: (example)</p> <ul style="list-style-type: none"> • Daily running of the service. • Provisioning of a high availability configuration • Availability and Continuity plan
Maintenance	<p>The internal supplier is responsible for (example):</p> <ul style="list-style-type: none"> • Bug fixing and proactive maintenance of the software • Documentation • Requirements gathering

4. Service hours and exceptions

IT services according to the service catalogue are delivered during 24 hours per day, 7 days per week (i.e. 365 days or 8,760 hours), to seamlessly support business operations. Planned and announced interruptions may reduce the effective operating time of a service.

The following exceptions apply:

- Planned maintenance windows or service interruptions (“scheduled downtimes”) shall be notified in a timely manner, i.e., 24 hours prior to the start of the outage, using a method appropriate for the service (e.g. email, banner, social media)
- Downtime periods exceeding 24 hours need justification.
- Human services are provided during support hours as defined below.

5. Support

Support is provided via the EOSC Future helpdesk support unit: <specify>

Support is available between:

- [Monday and Friday]
- [9:00 and 17:00 CET/CEST]

[This excludes public holidays in all organisations providing the service.]

5.1 Incident handling

Incidents will be handled according to the Quality of Support level that is estimated according to the impact of the outage or service quality degradation.

The Quality of Support levels are defined as follow:

Base level defines a response time of 5 working days regardless of the ticket priority.

Medium level:

Incident priority	Response time examples
Low	5 working days
Medium	5 working days
High	1 working day
Top Priority	1 working day

Advanced level:

Incident priority	Response time examples
Low	5 working days
Medium	1 working day
High	4 working hours

Response time is provided as service level target.

5.2 Service requests

In addition to resolving incidents, standard service requests (e.g. change requests, information requests, documentation) will be fulfilled through the defined support channels in the same way as incidents. Service requests are classified as “Less urgent”.

6. Service level targets

Monthly Availability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month.

- Minimum (as a percentage per month): 99%

Monthly Reliability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods
- Minimum (as a percentage per month): 99%

Quality of Support level

- Medium

7. Limitations and constraints

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in the following language: English
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure
 - Any party's failure to perform any term or condition of this Agreement as a result of circumstances beyond the control of the relevant party (including without limitation, war, strikes, flood, governmental restrictions, and power, telecommunications or Internet failures or damages to or destruction of any network facilities) ["Force Majeure"] shall not be deemed to be, or to give rise to, a breach of this Agreement.
 - If any party to this Agreement is prevented or delayed in the performance of any of its obligations under this Agreement by Force Majeure and if such party gives written notice thereof to the other party specifying the matters constituting Force Majeure together with such evidence as it reasonably can give and specifying the period for which it is estimated that such prevention or delay will continue, then the party in question shall be excused the performance or the punctual performance as the case may be as from the date of such notice for so long as such cause of prevention or delay shall continue.

8. Communication, reporting and escalation

8.1 General communication

The following contacts will be generally used for communications related to the service in the scope of this Agreement.

EOSC Future contact point	Matthew Viljoen matthew.viljoen@egi.eu
Service(component) owner contact point	The person from the organisation that is supplying the service
Support contact	The SU listed above

8.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the service, the following reports will be created as part of the service management. The service supplier is expected to provide necessary input for these reports:

Report title	Contents	Frequency	Delivery
--------------	----------	-----------	----------

Service Performance Report	The document provides the overall assessment of the monthly service performance and service level target performance achieved during last 10 months	Every 10 months	Document made publicly available via the public project wiki
----------------------------	---	-----------------	--

8.3 Violations

The supplier commits to inform the T7.4 task leader, if this Agreement is violated or if violation is anticipated. The following rules are agreed for communication in the event of violation:

- In case of any violation of the service targets, the Core supplier will provide justifications and a plan for services component enhancement to the T7.4 task leader. The Core supplier will produce a status report and a service component enhancement plan for the improvement of the service components within one month from the date of the first notification.
- The EOSC SMS supplier management staff will notify the Core supplier in case of a monitored potential violation via the EOSC helpdesk. The case will be analysed to identify the cause and verify the violation.

8.4 Escalation and complaints

For escalation and complaints, the Core supplier contact point shall be used, and the following rules apply:

- In case of repeated violation of the Services targets for two consecutive months or 4 months in a reporting period, a review of the Agreement and of the Services component enhancement plan will take place involving the parties of the Agreement
- Complaints or concerns about the Service components provided should be directed to the Core supplier contact who will promptly address these concerns. Should the EOSC Future project still feel dissatisfied about either the result of the response or the behaviour of the Core supplier, the TCB tcb@eoscfuture.eu should be informed.

9. Information security and data protection

The following rules for information security and data protection apply:

- While assertion of absolute security in IT systems is impossible, the Core supplier agrees to make every effort to maximize security level of users' data and minimize possible harm in the event of an incident
- The Core supplier must define and abide by an information security and data protection policy related to the service being provided
- This must meet all requirements of any relevant EOSC Future policies or procedures and also must be compliant with the relevant national legislation
- The Component Provider must comply with the EOSC Future Policy on the Processing of Personal Data[?] and provide a Privacy Notice. This Privacy Notice must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)
- The Component Provider must enforce the EOSC Future WISE Acceptable Usage Policies
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct in its most current version, which will be made available to the Component Provider by EOSC Future upon request

10. Responsibilities

10.1 Of the EOSC Core supplier

Additional responsibilities of the Component Provider are as follows:

- Adhere to all applicable operational and security policies and procedures, as well as to other policy documents referenced therein
- Use the communication channel defined in the agreement
- Attend T7.4 meetings and other operations meeting when needed
- Accept EOSC Core monitoring service provided to measure fulfilment of agreed service level targets

If delivering software as a service, the additional responsibilities of the Component Provider are as follows:

- A service with associated roles is registered in the Core topology
- Changes in the system must be rolled in production in a controlled way in order to avoid service disruption, following the Change Management within the EOSC SMS

10.2 Of EOSC Future

The responsibilities of the customer include:

- Raise any issues deemed necessary to the attention of the Core supplier provider
- Collect requirements from the customers
- Support coordination with other EOSC Future services
- Provide monitoring and helpdesk to measure fulfilment of agreed service level targets
- Create and provide service reports based on CPA

11. Review, extension and termination

There will be reviews of the service performance against service level targets and of this Agreement at planned intervals with the EOSC Future according to the following rules:

Technical content of the agreement and targets will be reviewed on a yearly basis

6 References

- [1] EOSC Service List, EOSC Future T7.4 Private Wiki
<https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Services> NOT AVAILABLE TO THE PUBLIC
- [2] SOCRM Procedures:
<https://wiki.eoscfuture.eu/display/EOSCSMS/Service+Order+and+Customer+Relationship+Management+-+SOCRM> NOT AVAILABLE TO THE PUBLIC
- [3] GOCDB for EOSC: <https://gocdb.eosc-portal.eu/>
- [4] EOSC Future Wiki: <https://wiki.eoscfuture.eu/>
- [5] ISRM Process:
<https://wiki.eoscfuture.eu/display/EOSCSMS/Incident+and+Service+Request+Management+-+ISRM>
NOT AVAILABLE TO THE PUBLIC
- [6] Level 1 Rota: <https://wiki.eoscfuture.eu/display/EOSCSMS/EOSC+Helpdesk+L1+Rota> NOT AVAILABLE TO THE PUBLIC
- [7] EOSC Helpdesk Guidelines: <https://wiki.eoscfuture.eu/display/EOSCSMS/Helpdesk+Guidelines>
- [8] ISRM1 Procedure: <https://wiki.eoscfuture.eu/display/EOSCSMS/ISRM1+-+How+to+Record%2C+Classify%2C+Prioritize%2C+Escalate%2C+Resolve%2C+Close+an+Incident+or+Service+Request> NOT AVAILABLE TO THE PUBLIC
- [9] ISRM2 Procedure for Major Incidents:
<https://wiki.eoscfuture.eu/display/EOSCSMS/ISRM2+Perform+a+major+incident+or+degradation+review> NOT AVAILABLE TO THE PUBLIC
- [10] EOSC Future Jira instance: <https://jira.eoscfuture.eu/>
- [11] EOSC Future Glossary: <https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Future+Glossary>
- [12] FitSM Standards Family: <https://www.fitsm.eu/>
- [13] EOSC-Hub Service Topology:
<https://docs.google.com/document/d/1iRURYnTeY8km7JEuw4nDu7g3c2dRvN4C6sKerebHhNQ/>
- [14] Minimum Viable EOSC. EOSC Architecture WG view on the MVE:
<https://data.europa.eu/doi/10.2777/492370>
- [15] D2.5a Inventory of Core Functions and Inclusion Criteria:
<https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Future+Project+Deliverables> NOT AVAILABLE TO THE PUBLIC