D4.3 Policies and Procedures for the Production Infrastructure

Lead Partner:	EGI Foundation
Version:	1
Status:	Approved by EC
Dissemination Level:	Public
Document Link:	https://documents.egi.eu/document/3500

Deliverable Abstract
This deliverable provides an overview of the operational processes, policies and procedures applicable to the services of the European Open Science Cloud (EOSC) Portfolios. This is achieved by providing a description of the proposed EOSC hub Service Management System including background of its development and plans for future activities.

OSC-HUB RECEIVES FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER RANT AGREEMENT NO. 777536.

COPYRIGHT NOTICE

DELIVERY SLIP

Date	*Name*	*Partner/Activity*	*Date*
From:	David Vicente Debora Testi Matthew Viljoen Alessandro Paolini Małgorzata Krakowian Owen Appleton Sy Holsinger Isabella Bierenbaum Pavel Weber João Pina Johannes Reetz David Groep David Kelsey Linda Cornwall	BSC CINECA EGI Foundation EGI Foundation EGI Foundation EGI Foundation EGI Foundation KIT KIT LIP MPG NIKHEF STFC STFC	5/09/2019
Moderated by:	Małgorzata Krakowian	EGI Foundation/Wp1	
Reviewed by:	Diego Scardaci Giacinto Donvito	EGI INFN	30/06/2019
Approved by:	AMB		

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v**0.1**	1/6/2019	Initial version with document structure	Matthew Viljoen
v0.2	17/7/2019	Contributions from all processes	multiple authors
v0.3	24/7/2019	Version ready for review	multiple authors
v0.4	30/7/2019	Incorporated feedback from reviewers	Matthew Viljoen
FINAL	5/09/2019	Final version	Matthew Viljoen

TERMINOLOGY

https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Glossary

Terminology in this document follows that which is defined in the FitSM-0 standard[1] [1], which includes full definitions. A glossary including common terminology for the EOSC hub project is also available[2]. Other terms used in this deliverable are listed here:

Acronym	Definition
AAI	Authentication and Authorization Infrastructure
AMB	Activity Management Board
AUP	Acceptable Use Policy
CSIRT	Computer Security Incident Response Teams
iRAT	issue (specific) Risk Assessment Team
RoP	Rules of Participation
SDT	Service Description Template
SMB	Service Management Board
SME	Small and Medium-sized Enterprise
SPF	Service Provider Forum
SVB	Service Validation Board
TRL	Technology Readiness Level
xGUS	EOSC hub helpdesk system

[1] FitSM Core Standard, including FitSM-0: https://fitsm.itemo.org/downloads/fitsm-core-standard/

[2] EOSC hub Glossary https://confluence.egi.eu/display/EOSC/EOSC+hub+Glossary

Contents

1 Introduction 6
2 Proposed approaches for Operations of the Production Infrastructure 7
2.1 SMS Portfolio scope and provider integration 7
2.2 The Service Management Board and Service Provider Forum 10
2.3 Onboarding of New Services 11
2.4 Implementation of the Onboarding Procedure 11
3 Policies and Procedures for the Production Infrastructure 16
3.1 Service Portfolio Management (SPM) 16
3.2 Service Level Management (SLM) 18
3.3 Order and Customer Relationship Management (SOCRM) 19
3.4 Service Reporting Management (SRM) 21
3.5 Supplier and Federation Member Relationship Management (SFRM) 22
3.6 Configuration Management (CONFM) 23
3.7 Change Management (CHM) 25
3.8 Release and Deployment Management (RDM) 29
3.9 Service Availability and Continuity Management (SACM) 30
3.10 Capacity Management (CAPM) 31
3.11 Information Security Management (ISM) 32
3.12 Incident and Service Request Management (ISRM) 34
3.13 Problem Management (PM) 35
3.14 Continual Service Improvement (CSI) 35
4 Conclusions 38
5 References 39

Executive summary

This deliverable provides an overview of the operational policies and procedures that have been developed within the EOSC-hub project in order to provide services within the EOSC Portfolios. It has attempted to provide a narrative of the different policies and procedures rather than a simple list of the policies and procedures themselves. This includes background covering the justification why they are needed, problems and challenges faced in creating them within the complex federated environment of the EOSC, and future plans for their further development.

The EOSC hub project has been given a remit to instantiate the first instance of the European Open Science Cloud (EOSC), a federated environment including a highly heterogeneous set of services intended for a wide range of users. At the same time, the EOSC needs to present these services in a consistent manner, making them easily discoverable, orderable and usable. The services themselves originate from a very wide range of different service providers, from the existing e-Infrastructures participating in the EOSC hub project to other e-Infrastructures outside the project including any other service providers wanting to join the EOSC. These can include service providers within specific research domains, small and medium-sized enterprises (SMEs) and researchers that have developed software that may be of value to others. Finally, the EOSC includes the services that EOSC hub delivers itself, including the EOSC Helpdesk and Marketplace - services which may not be ordered but are needed to operate the EOSC and may be adopted/integrated by/into external services.

Procedures and policies for the production infrastructure include those that have been developed as part of the EOSC hub Service Management System (SMS). Between those, the procedures and policies that have been developed for on-boarding external new services external to the EOSC Portal Service Catalogue and Marketplace take on great importance. It must be noted that the services external to EOSC -hub that have been onboarded are run by the service providers themselves and not by the EOSC and are not typically members of the EOSC hub project. As such, the procedures and policies within these organizations do not necessarily fall under the scope of anything being developed within EOSC hub.

1 Introduction

This document provides an overview of the operational processes, policies and procedures applicable to the services of the EOSC Portfolios. This is achieved by providing a description of the proposed EOSC hub Service Management System including background of its development and plans for future activities.

It is organised as follows:

- Section 2 presents the proposed approaches for Operations of the production infrastructure. EOSC Service Portfolios are described together with their relationship with the EOSC SMS. New boards of service providers set by the project for EOSC are introduced. The procedure to onboard new services in the EOSC is detailed.
- Section 3 provides an overall of the currently defined processes, procedures and policies supporting the delivery of services within the federation forming the EOSC hub.
- Section 4 includes the conclusions.

2 Proposed approaches for Operations of the Production Infrastructure

2.1 SMS Portfolio scope and provider integration

At the beginning of the EOSC hub project, it became clear that there were services with different characteristics:

- Federating core services provided by the participating e-Infrastructures, included in the original project proposal and project description of activities,
- Other services provided by the participating e-Infrastructures, and
- Services potentially interested in joining the Marketplace from service providers external to the project

In order to properly define the scope of the new Service Management System (SMS) and the scope of its different processes that were setup during the first year of the project, these different services needed to be properly organised in service categories and, consequently, into portfolios to ensure consistency and avoid confusion, both within the SMS and among the different service providers.

The resulting portfolios are:

- The Hub Portfolio: the internal services contributing to the federating core of EOSC, both for internal operation of the Hub (federation services), to enable the access to EOSC (access-enabling services) and to offer as components to be integrated into external Services.
- The EOSC Service Portfolio: the external services which EOSC hub either provides from its partners or onboards from the community to contribute to the larger portfolio of researcher-benefitting services within EOSC. Services in this portfolio can fall in two different categories: (1) thematic services, community-specific capabilities including research core data, data products, scientific software, and pipelines. And (2) common services, provide generic capabilities usable by any science discipline, each supporting aspect of the data lifecycle from creation to processing, analysis, preservation, access and reuse.

The Hub portfolio is defined as being in scope of the EOSC hub SMS, as these are the services we can control and govern, and whose quality we must manage. All processes will or may apply to these services.

For the external services we contribute to the EOSC Service Portfolio, the scope is less immediately clear. The definition of the **service package-based Rules of Participation (RoP) approach** described below attempts to clarify this aspect.

The initial attempt at categorization of service integration was covered in D4.1[3] and proposed three tiers of categorization, which were mapped to the level of integration: HIGH, MEDIUM and

[3] EOSC-hub Project Deliverables https://www.eosc-hub.eu/deliverables

LOW. Some services delivered by the service providers within the project (including the participating e-Infrastructures) were HIGH and service from newly onboarded external service providers were LOW. The anticipation was that external service providers who desire a closer level of interaction with the project (including technical integration) could transition to a MEDIUM level of integration, which would impose additional requirements on the maturity of their own SMS.

Although this three-tier service categorization and integration approach benefitted from simplicity, it also raised a number of questions: under what criteria a service may transition from LOW to MEDIUM as well as the dependency it had on the level of technical integration. It also suggested a fixed relationship between the level selected and RoP applied, whether or not this made sense in the specific situation.

An alternative system of service categorization was proposed and agreed within the RoP Taskforce[4]. It is based on *how* a newly onboarded service engages with the Hub - which depends on which "package" of federating service that the service provider chooses to make use of and integrate with their service. This **service package-based RoP approach** decouples the categorization of the services from the technical integration and allows different RoP to apply, depending on the nature of its engagement/integration with the EOSC hub. It moves away from a rigid RoP approach depending on the old 3 tiers and allows for the RoP to be dependent on the needs of the service.

At a base level, all onboarded services must be in the scope of EOSC hub SPM in order to be included into the Service Portfolio, and then publicly exposed in a Service Catalogue (in this case generally the EOSC Portal Marketplace). How the scope of other SMS processes impacts on new onboarded services depends on the choices the service providers make for using the Marketplace or integrating with other Hub Portfolio components. For example, enabling ordering will bring them partially into the scope of SOCRM, using the Helpdesk involves them in the ISRM process, and so on. Additional integration activities may bring the services within the scope of other SMS processes. This is shown in the diagram below.

[4] https://wiki.eosc-hub.eu/display/EOSC/AMB+Task+Force+on+Rules+of+Participation

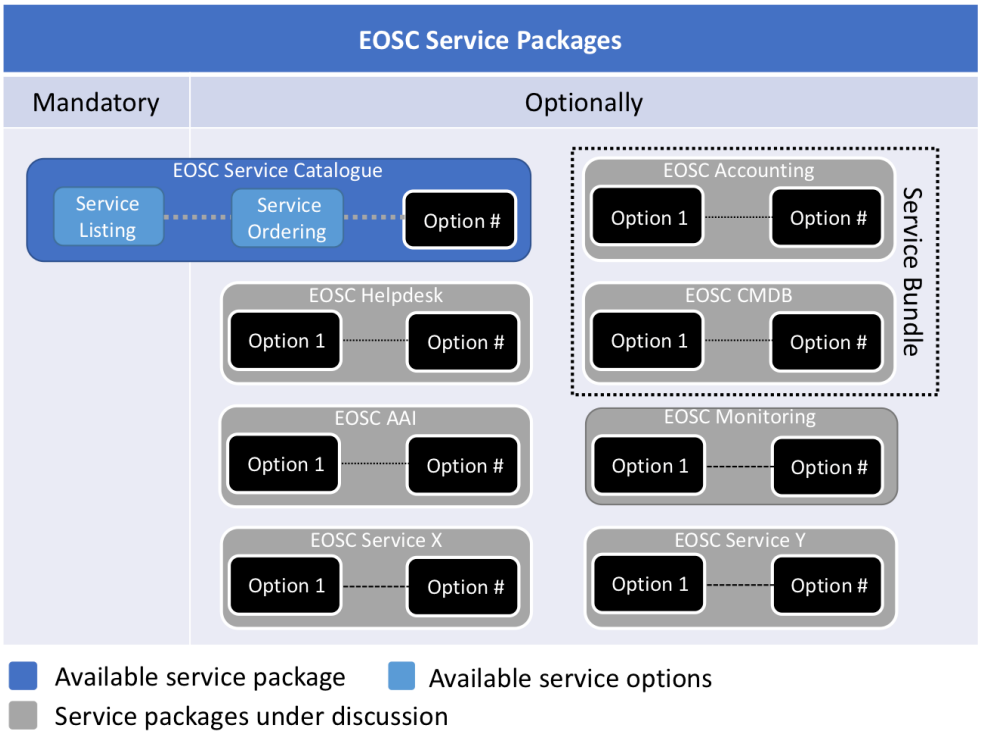


Figure 1: A simplified view of the overview of the EOSC hub Service Packages concept

Some examples will help to further illustrate this approach. Suppose that an onboarded external service wishes to make use of the EOSC hub Helpdesk service. The relevant RoP for the Helpdesk may require the service provider to provide a second line support entity, either with the helpdesk that the service provider may already be using, or integrated with the EOSC hub Helpdesk service. It may also make sense for the service to fall under the scope of the Incident and Service Request Management (ISRM) process of the EOSC hub SMS.

Suppose now that the same onboarded external service wants to make use of an EOSC Authentication and Authorization Infrastructure (AAI) service to aid its users with single sign on functionality. The relevant RoP for AAI may require the service provider to meet minimum security requirements and to accept the EOSC hub standard site security policy in order to ensure the secure exchange and processing of attributes of end users by the AAI.

We believe that this new approach sets the basis for a flexible method of on-boarding new services that meets the needs of EOSC to provide a consistent catalogue of production services while at the same time not burdening new service providers with unnecessary requirements. The package model is also the base to define a tiered partner schema, as described in the EOSC Portal concept paper[5] that would allow external providers to easily see the different ways they can profit from Hub Portfolio benefits, but also understand the related rules

[5] https://wiki.eosc-hub.eu/display/EOSC/EOSC+Portal

2.2 The Service Management Board and Service Provider Forum

Within the first year of the project it was realized that engagement with the different service providers of EOSC hub were necessary in a way that was not conceived with the structure of the EOSC hub project and in a way that can persist after the end of the project. This was as a result of the different requirements of setting up an effective project with a definite life and creating the foundations of a new infrastructure that will go on to form the EOSC itself.

A number of important needs were identified for such engagement with the service providers

- two-way communication between the project and service providers - involving project news, project developments and security announcements as well as requirements from service providers and their respective user communities - these being critical stakeholders for the success of EOSC hub and the future EOSC
- a way of soliciting input for aspects of operations that affect service providers including onboarding procedures and RoP
- maintenance of policies affecting service providers

Furthermore it was recognised that the nature of production delivery of service and federated operations within a future EOSC would ultimately be determined by the new governance structures of the EOSC including the new working groups charged with different aspects of the EOSC. Nevertheless, EOSC hub wanted to propose and implement an initial solution within the timeframe of EOSC hub that could then be evolved as necessary to meet the changing needs of the future EOSC.

It was proposed that a two-tier solution would be necessary since the needs identified above included executive and management aspects (e.g. maintenance of policies) as well as aspects of information dissemination and requirements gathering. With the evolution to the new service package-based RoP approach, it was decided that this may be achieved by the creation of two entities with the following composition:

- It is planned that the **Service Management Board (SMB)** is charged with maintaining federated operational procedures including RoP and policies. The SMB would be initially composed of representatives of the e-Infrastructures participating in EOSC hub - EGI[6], EUDAT[7] and INDIGO-DataCloud[8]. However, this could additionally involve representatives of other major stakeholders as appropriate.
- The **Service Provider Forum (SPF)** for project information dissemination and requirements gathering. The SPF would be initially composed of SMB as well as contacts from all external services onboarded into the catalogue. The primary mode of communication is a mailing list and face to face meetings can be held at project conferences or other EOSC

[6] EGI infrastructure https://www.egi.eu/

[7] EUDAT infrastructure https://www.eudat.eu/

[8] INDIGO-DataCloud project (INtegrating Distributed data Infrastructures for Global ExplOitation) funded under Horizon 2020. Original project website: https://www.indigo-datacloud.eu/

events. The first such meeting took place at the Service Providers' Bootcamp during EOSC hub Week in Amsterdam on Friday 12 April 2019.

2.3 Onboarding of New Services

The launch of the EOSC in Vienna on 23rd November 2018 included the announcement that new services could be added to the EOSC Catalogue and make discoverable on the EOSC Marketplace. For this to be possible, three main things were needed:

1. The criteria for which services were acceptable for inclusion onto the Service Catalogue and Marketplace and guidelines needed to be agreed and defined, including explaining what constitutes a sufficiently production-level service, by taking the generally accepted Technology Readiness Level (TRL) methodology[9] and adopting it for the EOSC

2. A Service Description Template (SDT) needed to be created containing the essential information needed from prospective Service Providers wishing to add their service to the EOSC Catalogue

3. The 'onboarding' procedure needed to be defined which covers the steps required to add new services to the EOSC Catalogue and Marketplace.

All of these points ultimately fall under the Service Portfolio Management (SPM) and the processes defined below. However, considering their relevance for EOSC hub, it is felt that they deserve more explanation. Parts 1. and 2. are fully explained in EOSC hub Project Deliverable D2.6[10]. An overview of Part 3. is included in D2.6 but its implementation is explained in more detail here.

2.4 Implementation of the Onboarding Procedure

Figure 2 Overview of service onboarding

[9] For more details and discussion about TRL please see Appendix II in EOSC hub deliverable D4.1 https://www.eosc-hub.eu/deliverables

[10] EOSC hub Project Deliverables https://www.eosc-hub.eu/deliverables

The EOSC Portal[11] is the first port of call for news relating to EOSC and accessing EOSC services and resources. It has been designed, developed and operated in the context of collaboration between EOSC hub and other EOSC projects, including OpenAIRE-Advance[12] and members of the former eInfraCentral[13]. On this website, providers of services are able to apply to participate in the EOSC by filling in a form (Figure 3) where essential initial information is requested about the service, reasons for wanting to become an EOSC provider, access conditions and contacts.

[11] EOSC Portal https://eosc-portal.eu
[12] OpenAIRE-Advance https://www.openaire.eu/
[13] eInfraCentral https://www.einfracentral.eu

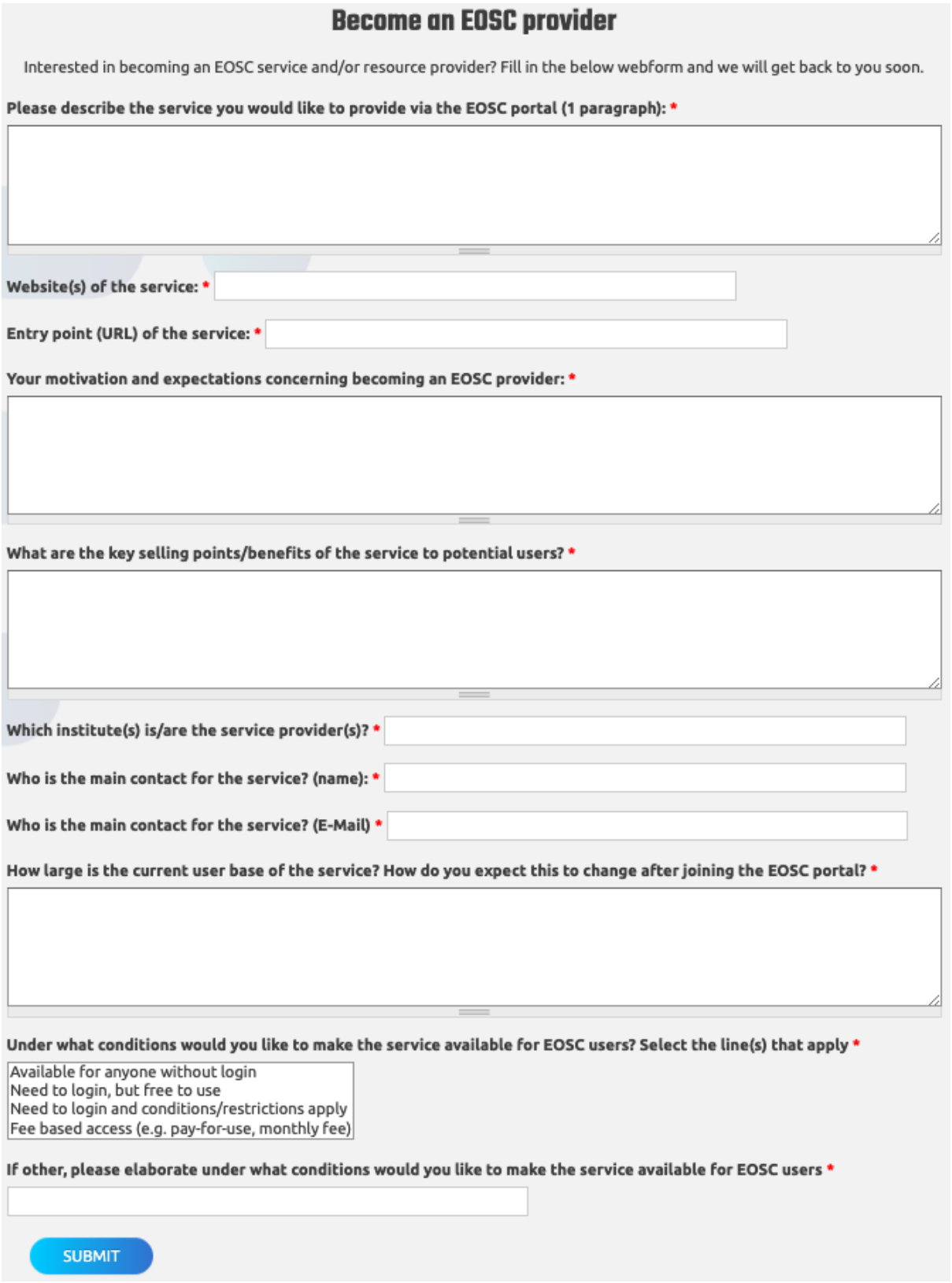


Figure 3 Initial form for interested service providers wishing to join EOSC

At the point of submission, this form results in the information being sent to a mailing list, upon which the information is initially reviewed before a Service Description Template (SDT) is created

for the requester who is invited to fill it in. The SDT (explained fully here[14] and also in the form of a collaborative spreadsheet which may be conveniently filled in by the requester) covers more detailed information which enables us to determine that the service fulfils all requirements of the Rules of Participation[15] as defined by the Rules of Participation Task force in addition to information needed to populate the Service Portfolio entry corresponding to the new service.

The addition of new services to the EOSC Catalogue and Marketplace is a very important activity and one that must be carefully considered to ensure that new services meet production requirements and are in alignment with the overall strategy of the EOSC. At the same time, it needs to be sufficiently agile to be able to cater for multiple service requests in order to grow the EOSC at a rate compatible with the expectations of stakeholders over the lifetime of the EOSC hub project, and to set in place the blueprint of a process that may be evolved after the project.

It is for this reason that a two phase onboarding process has been adopted - initial review of the information received and the final validation or approval of the request prior to publication of the service on the Service Catalogue and Marketplace. Both phases are manned by teams of people within the project who follow agreed rotas to ensure that there are constantly people available within the onboarding process.

2.4.1 Step 1 - Onboarding Request Review

This step is processed by a rota consisting of people from Task 4.1 Operations Coordination. This step includes reviewing the initial information submitted in the EOSC Portal form and checking the suitability of the request - that the service constitutes a service that falls within the remit of the EOSC hub activities (e.g. the request is not involving a plain dataset[16] or a software artefact and that if is a service, it is suitable for EOSC). A ticket is created in a dedicated Jira project and an SDT is created from the template in the form of a collaborative document, which is attached to the ticket and sent to the requester inviting him or her to fill it in. Once this is done, the completed information within the SDT is reviewed for completeness. This stage may involve a number of iterations with the requester, for example, if clarification is required in any of the information provided. It should be noted that this stage may take a number of weeks, depending on the responsiveness of the parties involved. As such, different people on the rota may deal with the same onboarding request.

2.4.2 Step 2 - Onboarding Request Validation

This step is processed by a rota consisting of people from Task 2.2 Service Roadmap, Service Portfolio and Service Catalogue. This step includes the final validation of the information within the SDT as well as the executive decision for the publication of the service on the Marketplace. As with Step 1, this step involves updating the Jira ticket associated with the request.

[14] Service Portfolio Entry Template https://wiki.eosc-hub.eu/display/EOSC/Service+Portfolio+Entry+Template

[15] Essential requirements for entry: https://wiki.eosc-hub.eu/display/EOSC/Service+Maturity+Classification

[16] Data-as-a-service can be onboarded in the Service Catalogue and Marketplace

Once these two steps is completed, the ticket is assigned to the Service Catalogue and Marketplace team for publication, initially on the development instance where the requester is invited to review the information about his or her service, and finally on the production Marketplace instance.

3 Policies and Procedures for the Production Infrastructure

In this chapter we provide an overview of the currently defined procedures and policies supporting the delivery of services within the federation forming the EOSC hub.

3.1 Service Portfolio Management (SPM)

Within the EOSC hub SMS, the SPM process manages two distinct portfolios. **The Hub Portfolio** comprises the internal services which empower EOSC hub, provide a 'minimum viable product' for a federated service landscape for EOSC, and offer functionality to be integrated into or to support the services in the other catalogue. These services are under the ownership and governance of EOSC hub.

The EOSC Service Portfolio contains services addressing EOSC customers; both single researchers and research communities. These include what EOSC hub foresaw as thematic services from single communities and also generic services which can support many if not all research communities.

The two portfolios are managed and governed in different ways. The Hub Portfolio is managed as a traditional service portfolio, with EOSC hub making strategic decisions about changes to it, which reflect customer needs, provider strategy and other factors. In contrast, the EOSC Service Portfolio is governed by EOSC hub, but its purpose is to include as many high quality research-supporting services from the community as possible. Hence the governance is about ensuring a base level of quality and clear description rather than selecting which services are included.

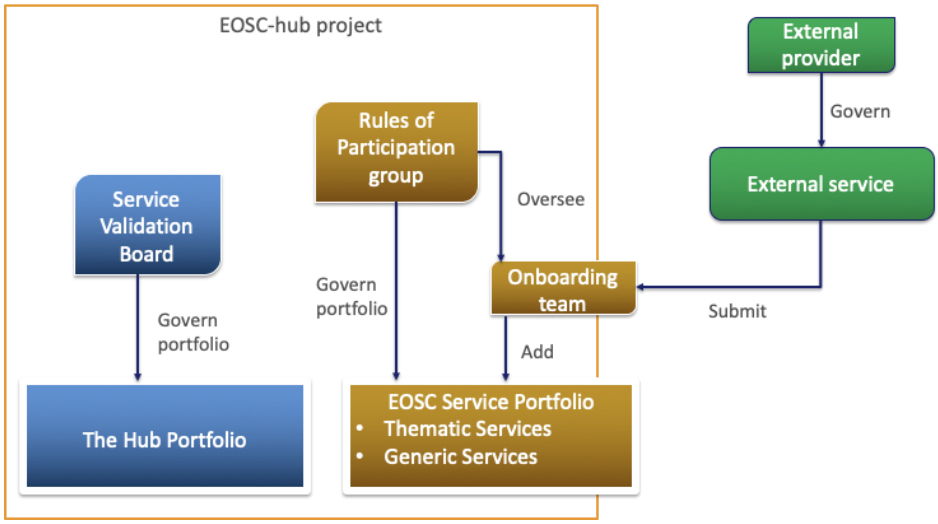


Figure 4. The two different service portfolios

For further details regarding the SPM Process and the rationale behind the two portfolios, please refer to EOSC hub project deliverable D2.6.

3.1.1 Policies

At present, SPM operates largely under the general Service Management Policy and the requirements of FitSM-1. SPM policies are in discussion in the Rules of Participation group as the approach to onboarding emerges from experience, and it becomes clear what can and cannot be required from service provider. These will appear in the coming months, but in the meantime the process operates sufficiently effectively.

3.1.2 Procedure SPM1 Add a service in the EOSC Service Portfolio

This procedure is the so-called 'onboarding' effort to take an external service and add it to the EOSC Service Portfolio. It involves a number of work packages collaborating to receive requests, gather data, validate it and publish a service. It is triggered from a form on the EOSC-portal site or by direct contact from a provider. It is then workflow-driven within Jira, using the following workflow.

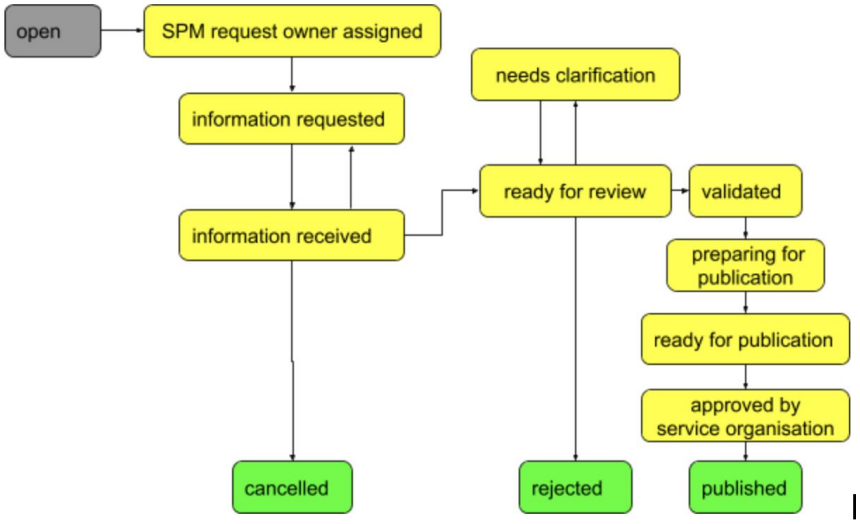


Figure 5. Onboarding workflow

Through this workflow, we move from a request to a well formatted, published entry in the Marketplace on EOSC-portal. Data is collected using a Service Portfolio Description Template, though later this may well be shifted to a dedicated tool for Service Portfolio Management. Some issues have arisen in this procedure related to the interfaces between teams but these are now being addressed.

3.1.3 Procedure SPM2 Change/retire a service in the EOSC Service Portfolio

This process is unusual, as changes to the service are made by the service owner, not by EOSC hub. Hence the change procedures are generally related to updating information about a service to reflect a change the provider has made, and are relatively simple. Services may be retired on request of the provider, but there is a need for a policy on when EOSC hub should retire a service from the portfolio unilaterally. We expect this to be a rare occurrence, but it should still be documented.

3.1.4 SPM3 Add or Retire a service in the Hub Service Portfolio

This procedure considers adding new internal services to empower the Hub or to allow for integration with them by EOSC Portfolios services. It is a more traditional SPM procedure, and is set within the governance structure seen in Figure 6 below.

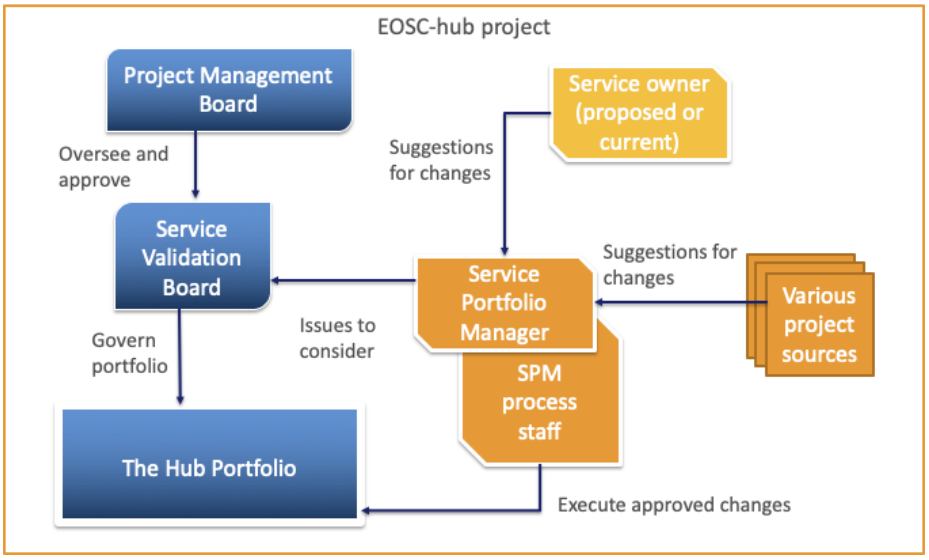


Figure 6. Proposed governance structure

The procedure is triggered from a number of sources, and moves to the Process manager, who coordinates the implementation of the procedure. The services are captured in a Service Design and transition package and considered by the Service Validation Board (SVB). Due to the political and strategic nature of these decisions, within EOSC hub additions and deletions from the portfolio will be passed to the Project Management Board for final decisions, based on Service Validation Board recommendations.

This procedure is relatively new as the project inherited an initial set of services that have not yet changes, but these must be reviewed, and new service suggestions are now starting to occur, hence the need to better clarify the terms of reference of the SVB.

3.1.5 SPM4 Modify a service in the Hub Service Portfolio

This procedure is almost identical to SPM, except that the SVB is charged with deciding whether the change is minor and can be taken at the SVB level, or major, and must be escalated to the PMB as with SPM3.

3.2 Service Level Management (SLM)

3.2.1 Procedure SLM1 Negotiate, sign, update, resign the Hub service participation agreement

This procedure is initiated once an internal supplier is identified by Supplier and Federated member relationship supplier in order to define and agree on a partnership agreement which will support delivery of service or service component belonging to The Hub service portfolio. The

outcome of this procedure, the agreement, is fundamental for providing the Hub. This procedure will be also used in case of agreement review which will take place every year. This type of an agreement is considered as an operation level agreement.

3.2.2 Procedure SLM2 Negotiate, sign, update, resign the EOSC service participation agreement

This procedure is initiated once a service provider wants to become part of EOSC service portfolio. This procedure covers negotiation and agreement between service providers and EOSC hub. The agreement will cover conditions under which the hub services will be provided to the service provider as well as responsibilities of the service provider towards EOSC hub.

This procedure will be also used in case of agreement review which will take place every year. This type of an agreement is considered as a service level agreement where the customer is a provider who wants to benefit from EOSC hub services.

3.2.3 Procedure SLM3 Manage EOSC service Participation agreement violation

This procedure will define communication and steps performed by EOSC hub in case of violation of the EOSC service participation agreement (see procedure SLM2). Goal of this procedure is that information is communicated and taken care of as defined in EOSC services participation agreement.

3.3 Order and Customer Relationship Management (SOCRM)

It is important to maintain an effective and continuous relationship between customers and service suppliers, and this is true for service suppliers providing services via the EOSC Service Catalogue and Marketplace.

Managing the relationship with customers is two-fold: to reply to customers' requests and orders and to monitor his/her satisfaction with respect to the ordering system. In this case, it is referred to the marketplace and orders management and not to the satisfaction of the single specific service which is monitored by the specific service provider and not part of WP4 activities.

The complete set of procedures and policies for Customer Relationship Management (CRM) are under completion but the basic concepts have been already agreed and CRM is already taking place at different levels.

3.3.1 Procedure SOCRM1 Service Order Management

The customer can, via the EOSC Service Catalogue and Marketplace, request access to one or more of the services provided by the different infrastructures. Due to the fact that the providers are many and that the type of requests might vary from a simple need to access to a required customisation, the procedure first of all differentiate three types of orders and the way how they have to be managed:

- request to access ready-for-use services: in this case, no authorisation is needed and thus the customer is redirected from the marketplace to the service web page for access;

- simple and well-defined order of one or multiple services: in this case, the shifter in charge of monitoring the incoming order will redirect the request to the corresponding service provider support;
- not well-defined order of one or multiple services: in this case, the shifter will first of all discuss with the customer to clarify the request and then forward it to the development/integration team.

The procedure is almost finalized for the first two types of orders, while for the third one there is still the need to better interface the procedure with the one related to the provisioning of technical support. In general, some work is also ongoing to reduce some of the manual actions and automate whenever possible the procedure.

At the end of the provisioning of any of the services, an important step is then to understand the customer satisfaction and get feedback on how the marketplace and services ordering can be improved in the future. This is at present managed by questionnaire performed by the different infrastructure and service providers (in particular EGI and EUDAT). An effort is ongoing to create a generic survey related to the services provisioning (not to the specific service satisfaction) and to submit it to EOSC hub customers periodically.

3.3.2 Procedure SOCRM2 Responding to EOSC hub 'Contact Us' requests

Besides sending orders for services or combination of services, customers can contact the EOSC hub team via the “contact us” form on the website.

The most important aspects covered by this procedure are the roles and actions to be taken by the team when a question arrives, and how to manage the different types of requests. In fact, some of the requests, like general information on how to access or ways to become providers, can be dealt directly, while others (i.e. questions on specific services or on technical issues) should be forwarded to the proper team into the project. In the first case, the team is supported by a set of frequently asked questions and answers. In the second case, the policy clarifies to whom the requests should be forwarded.

This procedure is managed in synergy with the stakeholder engagement activities.

3.3.3 Procedure SOCRM3 Recording and managing stakeholder information

Stakeholders are organisations outside the project consortium who can support project activities by e.g. becoming service providers; technology suppliers; users/consumers; or enablers (e.g. funding providers; policy or standard organisations). The database is used for entities where relationship management is needed before the case can enter the ‘usual’ procedures, such as service onboarding (if the stakeholder is a new provider), or service delivery (if the stakeholder is service customer).

This procedure defines how to record and maintain information about EOSC hub stakeholders in the Stakeholder DB. The Stakeholder DB is a database in the EOSC hub Confluence, with an entry form that helps the consortium record key information about the stakeholder, such as contact information, motivations, envisaged role in EOSC, what happened so far, what’s the next step, who is the owner in EOSC hub to manage the relationship, priority of engagement.

New stakeholders are typically added to the DB by members of 'T3.2 Stakeholder engagement' and by members of the AMB. The entries are owned by T3.2 and other WP3 members, and are reviewed periodically by the T3.2 task leader.

3.3.4 Procedure SOCRM4 Provide technical support

This procedure defines how to support those stakeholders who require technical assistance in consuming EOSC hub services. Technical assistance is provided by WP10, and it's triggered by the following events:

- SOCRM-01: a complex service order requires technical support. This typically happens when the customer needs to combine multiple services.
- SOCRM-02: request received through the contact form requires technical support. The case typically happens when a user is not sure which service(s) is/are suitable for his/her use case and a use case analysis is needed by someone who knows the EOSC hub services. In such cases the request arrives to EOSC hub through the 'Contact us' form instead as a service access order via the Marketplace.
- SOCRM-03: technical support is required for a newly engaged stakeholder to help it become a customer or provider in EOSC. This typically happens when a project member meets with a new user or user group at a meeting, workshop or conference and offers technical support for their use case.

Technical support typically starts with a teleconference meeting with stakeholders to better understand his/her use case, followed by an analysis by the WP10 team and then with the technical assistance delivered by owner of a (or multiple) services that are relevant for the given use case.

3.4 Service Reporting Management (SRM)

The goal of this process is to make sure that necessary reports are identified, defined, produced and distributed. The scope of this process are reports related to all SMS processes (supporting decision making regarding process effectiveness and efficiency) as well as service reports (supporting decision making regarding service effectiveness and efficiency).

3.4.1 Procedure SRM1 - Review a report catalogue and reports distribution

This procedure describes the steps which need to be taken to check if all reports are properly defined and the production and distribution of reports according to specifications take place. The goal of this procedure is to identify issues regarding report production e.g. report is in draft status for too long, report is not created and distributed as defined.

3.4.2 Procedure SRM2 - Define, update, terminate a report

This procedure defines steps to add, remove or update process report. Its goal is to ensure that information about change in reports are being taken care of and communicated properly.

3.4.3 Procedure SRM3 - Initiate follow-up actions in case of inaccurate reporting

This procedure describes escalation and communication steps in case of nonconformity with report definition for process reports. It is initiated by SRM1 in case of issues with reporting. Goal of this procedure is to properly follow up situations where reports are not or wrongly produced. It ensures that proper communication is taking place and finally the report is being produced or definition updated.

3.5 Supplier and Federation Member Relationship Management (SFRM)

Although EOSC hub is a project rather than a federation in the traditional sense, it is helpful to consider the existence of 'federation' members which are defined as the participating e-Infrastructures within the project (EGI and EUDAT) in addition to the INDIGO-DataCloud. These federation members themselves have service suppliers (apart from INDIGO-DataCloud which may itself be considered as a supplier of software) that provide services to end users and to the EOSC hub project. It is the responsibility of the federation members to manage agreements with their suppliers in the form of OLAs. Although delegation of this task is requested by the EOSC hub SMS, the activity itself is out of scope of the EOSC hub SMS, and instead takes place within the respective SMSes of the federation members.

The SFRM process has the aim of ensuring that a good relationship is maintained with the federation members, as described above, for the good of the project and to provide a basis of delivering production services within EOSC hub. This includes services both within the Hub portfolio and the EOSC portfolio. The primary driver for this is to ensure that the delivery of services by the federation members is not jeopardized by a breakdown of relationship, but it could potentially be extended to necessary information for maintaining a good relationship is the list of contact information for the different federation members - this information is stored within the SFRM Database.

Disputes, if and when they arise, are recorded in the SFRM Dispute Database. Each entry in this database includes information about the affected service or services, the supplier involved in the dispute, the person responsible for resolving the dispute and supplementary information.

3.5.1 Procedure SFRM1 Manage contractual disputes between the service provider and suppliers

This procedure describes how and when disputes should be recorded in the SFRM Dispute Database, including the type of information that should be recorded.

3.5.2 Procedure SFRM2 Maintain the supplier and federation member database

This procedure describes when and how the SFRM Database should be updated.

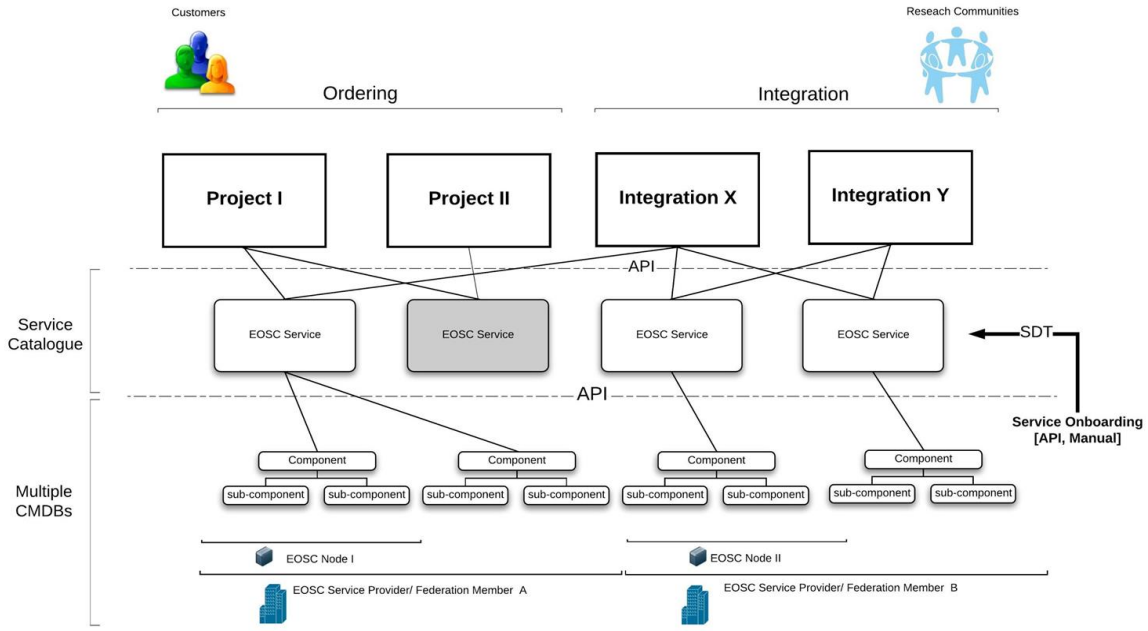
3.6 Configuration Management (CONFM)

The Configuration Management is the process that ensures the correct implementation of all policies, procedures and management tools necessary to monitor and implement many of the EOSC hub 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). So CONFM is a pillar for the whole SMS and in order to implement and run this process, it is necessary to keep the logical model together with the relationships and dependencies for all parts involved. To store this information, an initial schema of a distributed Configuration Management Database (CMDB), currently consisting of the GOC-DB of EGI and the DPMT of EUDAT, was defined and is now under implementation. A series of procedures was created in order to rule how the information should be handled. These procedures are critical in order to keep the CMDB in a coherent state.

Regarding the CMDB design, it is currently under evaluation and the planned configuration items (CI) are the following:

- Project (arbitrary grouping of existing services that can be distributed across different service providers);
- SLA (service level agreement signed between service provider and users)
- Service (single entity formed by a single service component or multiple service components);
- Service provider (EGI and EUDAT);
- Service Components (a single entity with several properties);
- 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).

In Figure 7 we can see how the proposed relationships between the CIs could be implemented for the EOSC hub CONFM:



One open question in this context and strongly discussed is how to propagate information about planned changes on configuration items across different federations.

3.6.1 Procedure CONFM1 Adding or removing a Configuration Item in the CMDB

This procedure describes how a Configuration Item is added or removed from the CMDB. The procedure can be triggered either by the SPM process or by the CI owner. Since the EOSC hub CMDB is a distributed database, the first step of the procedure is to guide the CONF Manager, the person responsible for implementing this procedure, to the component of the CMDB the CI is supposed to be stored in and to the rules defined there, which have to be followed.

3.6.2 Procedure CONFM2 Updating information in the CMDB

This procedure describes how to update information in the respective CMDBs (after a change) and is triggered when Information, Version or attribute on a Configuration Item, has been changed and needs update.

3.6.3 Procedure CONFM3 Taking a Configuration Baseline before a new release

This procedure describes how to take a Configuration Baseline before a new release will be implemented and is triggered by the Release and Deployment Management process when a new release is being prepared. This process is implemented by automatic procedures (regular backups of the DB) when CIs are changed.

3.6.4 Procedure CONFM4 Verifying information stored in the CMDB on regular intervals

This is a very simple procedure just to Inform/remind CI Owners to check and if necessary update the information on their CIs in the respective CMDB at regular intervals.

3.7 Change Management (CHM)

The EOSC hub Change Management policy is distributed over three areas for easier overview and linking purposes: the main Change Management Policy, the Types of Changes and the Change Advisory Board. The procedures CHM1 to CHM9 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, their roles defined by FitSM respectively. These steps of actions are implemented in the EOSC hub CHM JIRA project.

In a federation environment like the EOSC hub, some services are shared by several providers and thus fall under the scope of more than one Change Management, like for example the Operation Portal provided by EGI and used by both EGI and EOSC hub. During the first year of the project, this situation caused some interference on the EOSC hub CHM and it was necessary to tackle it. Therefore, a set of new policies and procedures were established between all providers (EGI/EUDAT and INDIGO), how to handle these cases, with the possibility of extending to further providers or services. It should also be mentioned that the EOSC hub CHM scope was enlarged and is now focused on both the core and the production infrastructure, increasing the number of services and the complexity of the CHM process.

Another point to be taken into account in the future work of this process is the starting point from which a change on a service should be monitored by the CHM. Should a change be registered and monitored from the very beginning, like for example the user/community request, or at a later point during the development stage. In the current implementation, a change is monitored by the CHM process after it has been checked for technical feasibility and been validated by the work packages WP5 and WP10. The CHM becomes involved afterwards by the creation of a Request for Change (RfC) in form of a ticket in the CHM JIRA project.

The future work foreseen for the EOSC hub CHM will also take into consideration the post project lifecycle where references to work packages does not make sense anymore. In this context, the challenge will be to track the development of services and provide sustainable procedures for change approvals in an environment like the EOSC with many different service providers and infrastructures.

3.7.1 Policy Change Management Policy

The Change Management Policy is the main point of reference for the EOSC hub Change Management. It contains the basic information and general rules that underlie this process. In this policy, the variables needed in the following, such as the Request for Change (RfC) and the roles of people involved (the Change Requester, Owner, Implementer, etc) are defined and links are provided to the Types of Changes and the Change Advisory Board.

3.7.2 Policy Types of Changes

This part of the policy introduces the three types of changes which are defined following FitSM: Standard, Non-Standard and Emergency Changes, where the Non-Standard Changes are further refined into Normal and High-Risk Changes. All changes differ in general by their risk-levels,

approval and review steps, and involved entities. The idea behind this splitting of changes into different types is to generate a flexible and easy-to-interact CHM, which still keeps a maximum of safety for the SMS, when changes are applied. The Emergency Changes allow people to immediately act on security events, without being stopped or delayed by a CHM approval. The Standard Changes provide the opportunity to put recurring changes on a list of pre-approved Change Requests, such that repeating changes with the same structure can be processed more easily, omitting unnecessary delay and workload. The splitting of Non-Standard Changes into Normal and High-risk accommodates different risk-levels of proposed changes, where low-risk changes can be checked by CHM staff members, whereas high-risk changes need an approval of the Change Advisory Board.

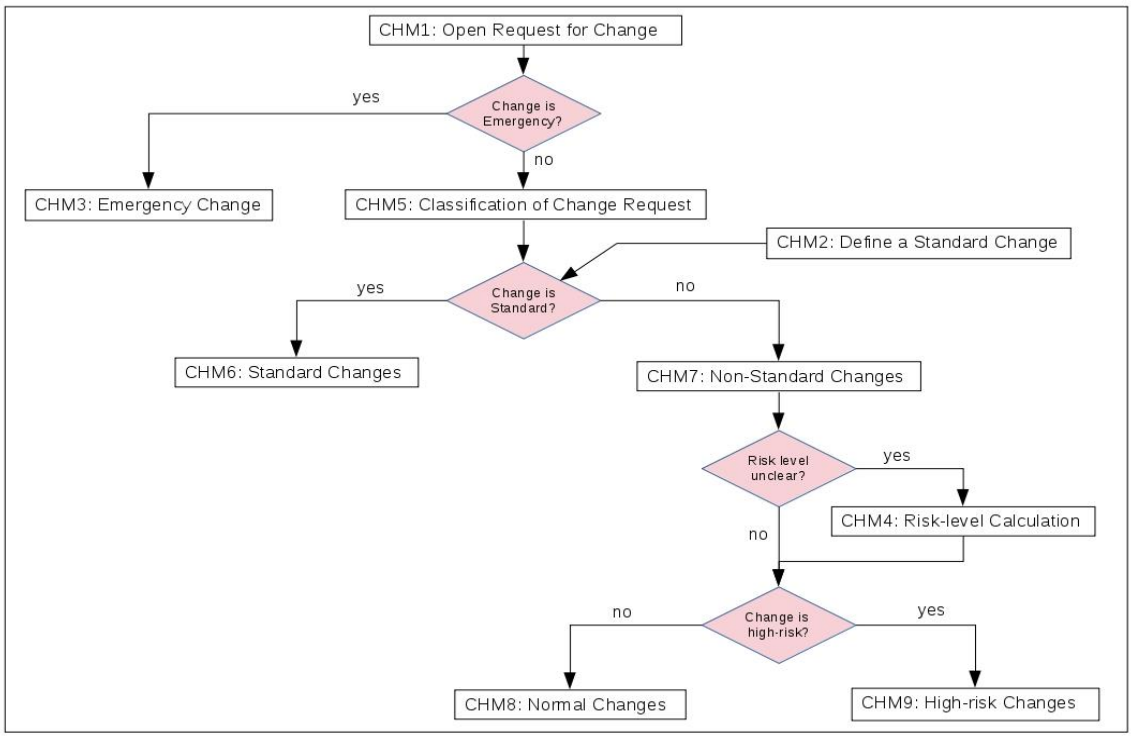
3.7.3 Policy Change Advisory Board

The Change Advisory Board (CAB) is built as a board of experts addressing important issues related to Change Requests. This can for example be an RfC, whose risk level is high and which can have a major impact on the SMS in case the implementation fails. The policy states the people constituting the board, the responsibilities of the CAB, as well as meeting formalities. In case of need, the CAB can invite external experts in order to correctly assess a change with its risks and impact. The board members are approved by the EOSC hub Activity Management Board (AMB) and the CAB currently consist of representatives from EGI, EUDAT and INDIGO.

3.7.4 Procedure CHM1 Open a Request for Change

All changes are implemented in the EOSC hub CHM JIRA project. The corresponding workflow is triggered by the Change Requester opening a Request for Change (RfC), a ticket in the JIRA project respectively, which is described in this procedure. Inside the JIRA project, the ticket is then sent into the correct workflow (emergency standard, normal or high-risk). All further status changes are performed by an assigned Change Owner from the CHM staff, with some interactions by the Change Implementer (like the start of the implementation, as well as its end and outcome). All changes include a review process. A JIRA dashboard has been created which tracks the tickets in its various steps.

This procedure aims at guiding the Change Requester through all steps necessary for opening a ticket. To this extent, a table is provided with information on the fields required to be filled in the JIRA ticket. Additionally, a link to the CHM JIRA project is given. The current Procedure 1 actually starts with the question, whether the change at hand is an emergency change. If yes, one should immediately continue with Procedure 3.



All procedures, this and the following, describe the workflow implemented in JIRA in the form of steps, where the actions of the entities and their roles (defined by FitSM) are stated. The following diagram shows an overview over the EOSC hub CHM procedures implementing the policies and current workflows for all types of changes, where the names of the procedures have partially been adjusted for better readability.

3.7.5 Procedure CHM2 Define a Standard Change

The EOSC hub CHM provides a list of Standard Changes, which are changes of a particular type, which will be implemented repeatedly (e.g. regular maintenance updates of installed software). These changes are approved once by the CAB, put on the List of Standard Changes, and are then pre-approved for future occasions. The Change Requester can contact the CHM and ask for his/her change to be put on this list. The procedure describes the steps which have to be taken to accomplish this. The List of Standard Changes is visible on the Confluence page, where a description of the respective change is provided.

3.7.6 Procedure CHM3 Manage Emergency Changes

Emergency Changes allow the Change Requester to implement a change without prior approval by the CHM process. This can be done to resolve a critical situation, where time is a pressing issue. However, after the change is implemented, it is required that a ticket is opened to inform the CHM process of this event and to allow the CAB to perform a post-implementation review. This procedure describes the emergency situations in more detail, as well as the workflow latter implemented in JIRA.

3.7.7 Procedure CHM4 Calculate the Risk Level

In order to classify a change correctly according to its risk level, one needs to perform a standardized risk analysis. To this extent, this procedure states the necessary steps and links to a risk management page, where the risk level of a change can be deduced by evaluating its risk likelihood and risk impact, and afterwards consulting a risk matrix. There are four different risk levels stemming from this assessment: low, medium, high and extreme. These levels are used in the subsequent procedures to classify changes and to send them into the correct workflow. The risk analysis should primarily be performed by the Change Requester when opening the ticket, where he/she mandatorily has to fill fields on the risk likelihood, risk impact and risk level ("unknown" is a valid option).

The current definitions for the risk analysis for opening a Request for Change are under discussion and will be refined and adapted for the EOSC hub ecosystem.

3.7.8 Procedure CHM5 Classify a change as Standard or Non-Standard

After a Request for Change has been opened according to Procedure 1 and if the change is no emergency change, this procedure describes the next step, the classification as Standard or Non-Standard Change. If the change is on the List of Standard Changes, Procedure 6 is called. Otherwise the change is classified as Non-Standard and the workflow continues with Procedure 7.

3.7.9 Procedure CHM6 Manage Standard Changes

If an RfC has been opened and the change has been classified as Standard Change following Procedures 1 and 5, this Procedure 6 describes the subsequent steps for this type of change, as they are implemented in the JIRA workflow. However, since Standard Changes are pre-approved by the CAB, there is no approval step in this workflow.

3.7.10 Procedure CHM7 Evaluate the risk level for Non-Standard Changes

If an RfC has been opened and the change has been classified as Non-Standard Change following Procedures 1 and 5, it is necessary to further classify the change as Normal Change or High-risk Change, according to its risk level. If the risk level was already correctly assigned by the Change Requester, changes of low or medium risk level continue with Procedure 8, while high- or extreme-risk changes continue with Procedure 9. In case there was no risk level assigned to a change by the Change Requester, the Change Owner responsible for this ticket has to classify the change at this step, making use of Procedure 4.

3.7.11 Procedure CHM8 Manage Normal Changes

Changes classified as Normal Changes (following Procedures 1, 5 and 7) can be approved and reviewed by an assigned Change Owner from the CHM staff without any involvement of the CAB. This procedure describes the steps from the approval of the change, through its planning phase (Awaiting Implementation), the actual Implementation and the subsequent Change Owner Review, to the Closed status. It also states, which steps (status changes) should be performed by the Change Owner and which steps need an action from the Change Implementer (the Change Requester respectively).

3.7.12 Procedure CHM9 Manage High-risk Changes

Changes classified as High-Risk Changes (following Procedures 1, 5 and 7) need to be approved and reviewed by the CAB. As in Procedure 8, the steps from the opening of the ticket through the workflow with the interactions of the Change Requester (Implementer), the Change Owner and the CAB are described.

3.8 Release and Deployment Management (RDM)

The goal of Release and Deployment Management is to plan and oversee the implementation of approved changes into production. This is done by defining a RDM policy which provides standardized ways of planning releases.

The RDM also offers a set of guidelines, procedures and best practices for EOSC hub service providers to manage their releases. This aims to promote the adoption of Software Quality Assurance (SQA) best practices for services releases within the EOSC hub aiming at the improvement of the Quality Of Service offered by EOSC hub.

The RDM operates in conjunction with the CHM. All results of the RDM are tracked in JIRA under the Change Management project where a dedicated dashboard has been created in order to better track the process implementation.

3.8.1 Policy Release and Deployment Management policy

The RDM policy supervises all changes to IT resources, services and / or systems approved by the EOSC hub Change Management. This policy requires that all changes to services should provide a release plan that includes release dates (testing period, and expected deployment in production), release notes and documentation for users and administrators together with a contingency plan. Additionally, this policy also enforces that all releases should be tested prior to implementing and evaluated after implementation.

3.8.2 Procedure RDM1 Internal Catalogue release and deployment process

This procedure describes the process of release and deployment of services present in the EOSC hub Portfolio and it is triggered by the Service Owner once the change requests go to Awaiting Implementation under the Change Management queue. The procedure consists of a series of sequential steps that Service Owners, providers and the EOSC hub operation team need to follow in order to properly deploy a new version of services.

In this procedure, the Service Owner’s responsibility is to properly prepare the release by defining in advance a testing and rollback plan together with accurate release notes and a functional testing service. The EOSC hub operation team has the responsibility to inform the relevant parties (users, other services, etc.) about the upcoming release. Finally, the Service Provider, like EGI or EUDAT, is the one that will inform the Service Owner to deploy the release and put in production. In the end, a post implementation report should be filled by the Operation team in collaboration with the Service Owner and annexed to the original change request.

3.9 Service Availability and Continuity Management (SACM)

In order to avoid duplication of work and overlapping with the participating e-Infrastructure SMSes, it was agreed to limit the SACM scope to only the (internal) services operated directly by the EOSC hub project; instead the services belonging to EGI and EUDAT will be under the control of the related participating e-Infrastructure, who will be responsible for their monitoring and to produce Availability and Continuity (A&C) plans according to the guidelines provided by the correspondent EOSC hub process (unless differently agreed for a particular service).

At the moment of writing, there are 2 finalised procedures in the process.

3.9.1 Procedure SACM1 Manage an event of a major loss of service

This procedure describes the actions to undertake to ensure the service continuity when it occurs an event of major loss of service. In such situations the ISRM manager notifies the SACM manager about a major incident affecting one or more services. Then the SACM manager assesses if the incident can be addressed by the availability and continuity plan in order to restore the service in a timely manner. Either if the A&C plan is enough to restore the service or not, it should be performed some investigations on what produced the incident in order to reduce the eventuality of future occurrences: new risks should be identified and defined, the countermeasures already in place should be reviewed and improved, new countermeasures should be defined, all of this (according to procedure described in the next section) with the purpose of reducing the related risks. In case these investigations trigger a change in the SAC plan, then also a new A&C test is required.

3.9.2 Procedure SACM2 Create and maintain Service Availability and Continuity plans

This procedure defines the creation and the maintenance of Service Availability and Continuity plans.

When an SLA for a service has been created or has changed, when the service level targets have been changed, then it is triggered the creation (or update) of the related service A&C plan. A list of potential availability and continuity risks are identified and the service provider is asked to perform the risk assessment by rating the risks level (in terms of likelihood and impact) in according to the risk evaluation criteria and by reporting some information like the measures already in place to mitigate the risks occurrence. The Service Owner and the SACM manager review the provided information trying to identify any remaining vulnerabilities and in case the countermeasures and/or the risk level are not considered acceptable, they will agree with the Service Provider solutions for reducing the impact and/or the likelihood of the risks.

Once the risk assessment is concluded, it is evaluated the need of a continuity test (depending on the critical level of the service), whose details will then be discussed with the provider: if the test is considered successful (compared to the A&C requirements for the service), then the plan can be finalised, otherwise one or more of the previous steps can be reiterated. After the plan is finalised, it is linked to the service OLA (and in case the service OLA itself is updated to reflect the service

A&C plan outcomes. It is also performed a periodic review of the several plans (generally on a yearly basis).

3.10 Capacity Management (CAPM)

The Capacity Management process has been defined based on the experience gained in the corresponding EGI process: in a federated and distributed environment where we operate, many services are usually not under our direct control but are managed by the service suppliers themselves, which they offer their services to the EOSC communities through the participating e-Infrastructures (the federation members). So that it is the service supplier that will take final decisions on service capacity aspects, and the role of the e-Infrastructure is the one of collecting and providing capacity requirements (releasing in case additional funding related to specific projects), which will then be used by the service suppliers to evaluate changes to the capacity of their services.

Besides these considerations, CAPM has been scoped following the same criteria of SACM, meaning that the federation members will take care of producing capacity plans for their services following the EOSC hub recommendations, while only a subset of services in the EOSC hub catalogue will be under the scope of the EOSC hub CAPM process.

3.10.1 Procedure CAPM1 Create and Maintain a Capacity Plan

This procedure describes the process for creating and maintaining a capacity plan. It is an important process allowing to assess the current capacity of a service compared to the current demand and usage of the service, and to plan changes to the capacity over a defined period based on forecasts of future demand.

When a service reaches the phase of being tested publicly, this is usually the moment to plan its capacity. The service business case design is reviewed by the Service Owner and the Capacity Plan Owner, considering aspects like demand, expected cost and expected revenue, service requirements and service acceptance criteria. For each service component defined in the SDTP, the capacity needs and performance (in terms of Service Level Targets as defined in OLAs/SLAs) are evaluated and it is also defined Service Level Indicators (SLI) and Service Level Objectives (SLO): a defined quantitative measure of some aspects of the level of service that is provided. Typical SLIs take into account technical aspects (like service usage and hardware consumption) and human ones. For each SLI, the data source and means of monitoring are specified.

With all this information collected, the Capacity Plan Owner can then define the strategy to adopt to respond to changes in utilisation of the given service, making some assumptions and putting in place thresholds to the several SLIs. Capacity can be adjusted in general with four strategies:

- Lead: adding capacity in anticipation of an increase in demand. The total capacity for the given service will be estimated and will be chosen to always be higher than anticipated demand.
- Lag: Waiting until the current capacity is stretched to its limits before adding more capacity.
- Incremental: Adding capacity in small increments when approaching full capacity.

- Dynamic (Predictive): Adding capacity, large or small, before it's required based on forecasts.

Once agreed on the capacity adjustment strategy, the Capacity Plan Owner will estimate resources and related costs necessary for the Capacity Plan implementation, reporting also if it is required an immediate change to the capacity in case this is considered insufficient to respond to the current (and short term) demand of the service. The Capacity Plan is then completed and ready to be discussed with the EOSC hub Management for the approval or rejection.

3.10.2 Procedure CAPM2 Approve Capacity Plan

Once a Capacity Plan is created, or an existing one has been updated, this needs to be discussed with the management to take financial decisions about the affected service. In our case, the Capacity Plan is presented first to the Project Coordinator who will evaluate if the request has a potential for major financial consequences for the EOSC hub: if not, the approval (or rejection) of the Project coordinator is enough to finalise the Capacity Plan. Otherwise, the request needs the Project Office approval (the decision will be the outcome of a formal vote). In case the management proposes some changes to the Capacity Plan, then Procedure 1 and 2 will be reiterated.

3.11 Information Security Management (ISM)

The Information Security Management process requires policies and procedures to ensure consistent and coordinated security operations across the services provided in the catalogue. Security activities are based on the policy framework, complementing the security best practices implemented by the individual service providers. When complete, this should include operational and incident response, participant responsibilities, traceability, legal aspects, and the protection of personal data. The policies and procedures are designed not to interfere with the local security best practices implemented by the individual service providers, but builds on them to ensure collaboration and uniform interoperation between service providers.

The security team also builds trust and creates effective interoperability with the actors outside of the project such as other e-Infrastructures (like GÉANT[17]), Research Infrastructures, and when appropriate, with dedicated security groups in Europe (TF-CSIRT[18]) and in the US, for example REN-ISAC[19], and at the same time actively participating in the activities of international initiatives such as WISE[20].

Future work to produce new policies and procedures is not yet fully agreed, but is likely to include:

- Data protection and privacy policy framework (GDPR)
- Control of workload activities to replace old EGI policies on Virtual Machines and Research Community portals

[17] GÉANT https://www.geant.org/

[18] Taskforce Computer Security Incident Response Teams, https://tf-csirt.org/

[19] Research & Education Networks Information Sharing & Analysis Center (REN-ISAC), https://www.ren-isac.net/

[20] WISE Information Security for E-infrastructures community, https://www.wise-community.org/

- Adoption of the WISE policy template policies on Research Community operations and management

3.11.1 Policy EOSC hub Security Policy

This is the overall “top-level” ISM policy. This document presents the policy regulating those activities of participants related to the security of the Collaborating Infrastructures within EOSC hub. The security policy is aimed to be compliant with WISE Security for Collaborating Infrastructures (SCI) version 2[21].

It will need to be revised and updated when/if additional policies are produced.

3.11.2 Policy Acceptable Use Policy and Conditions of Use

In defining acceptable use and setting the conditions of use, we apply a globally-coordinated template Acceptable Use Policy (AUP), namely the "WISE Baseline Acceptable Use Policy and Conditions of Use", template version 1.0, dated 25 Feb 2019. Any Service, Authentication system (AAI), or community membership management system, which presents the AUP to a user during their first use and registration, must adopt this template for their particular use case. Further guidance on how to apply the template AUP is available from the AARC[22] community (based on the EU H2020 project) in AARC-I044 (https://aarc-community.org/guidelines/aarc-i044/).

A policy based on this template must be applied to all users of any EOSC hub registered Service that is defined to be within the scope of the ISM process.

3.11.3 Policy EOSC hub Service Operations Security Policy

This ISM policy applies to Service Providers that operate any EOSC hub registered service within scope and expresses the expectations and requirements for security-related aspects of deploying and operating their service.

3.11.4 Procedure ISM1 Security Incident Response procedure

This procedure is aimed at minimizing the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Service Providers and Infrastructures. It is essential for the proper handling of security incidents and defines the actions that need to be taken by the IRTF and the participants involved.

This is a mature procedure but will be under regular review and will be revised as needed based on experience.

3.11.5 Procedure ISM2 Software Vulnerability Handling Procedure

This is a procedure for handling reported software vulnerabilities which are relevant to Services in scope. This is a complex multi-step procedure which has evolved from earlier simpler procedures, because of the ever-growing diversity of environments and software deployed. The current

[21] WISE SCI version 2 framework, https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

[22] AARC https://aarc-project.eu/

Software Vulnerability Group (SVG) team cannot be experts in all software, services and configuration in the EOSC environment. This leads to the biggest change in the procedure, the creation of an issue (specific) Risk Assessment Team (iRAT) for each issue reported. The iRAT consists of appropriate experts on software and its deployment in the various services who are invited to handle each issue reported. We are also likely to develop some sub-procedures of this Software Vulnerability Handling procedure, including the formation of the iRAT which will be refined based on experience, as well as possibly split this one large procedure into several simpler, more compact procedures that reference each other. This could be much simpler to maintain in future.

3.11.6 Procedure ISM3 Information assets, threats, security risk assessments and controls

Procedure to identify Information Assets and threats; to perform Security Risk Assessments; and to produce security controls. This is an important procedure related to carrying out risk assessment. The details as to how to create appropriate controls once a risk assessment is complete are still being discussed and the procedure will be modified to reflect our decisions as to how best to operate this.

3.11.7 Procedure ISM4 Approval and adoption of ISM Policies

Procedure for the consultation on, followed by formal approval and adoption of Security Policies. This is currently work-in-progress as the proposals as to how to carry out consultation and approval are not yet finalised. We will work on this more during the coming year.

3.12 Incident and Service Request Management (ISRM)

3.12.1 Procedure ISRM1 How to handle incidents and service requests through the ticketing system

The procedure defines all the steps required to handle a request or incident received in the EOSC hub helpdesk system (xGUS) until its final resolution. The procedure explains how to categorize, prioritize and escalate the requests/incidents to the different support units. This procedure is also including a link to the User support guidelines, which include information about the different categories, which means each of the priority levels and which are the steps and comprobations needed before escalating a request to the corresponding support unit.

Future Work: For the procedure, the ISRM team is working on improving the User support guidelines in order to re-define the priority levels and when the incident owner needs to increase its priority. In addition to this, the team is working on improving the information included in the guidelines, in order to provide more information for the 1st level support team to properly handle any request received in the xGUS ticketing system.

3.12.2 Procedure ISRM2 Creation of a new service unit in the EOSC hub helpdesk

This procedure defines how to create a new support unit in the EOSC hub helpdesk. Any new service to be handled by the EOSC hub helpdesk needs the creation of its own user support unit in

the xGUS service and the assignation of a responsible to handle the request escalated to this new support unit. The responsible can be a person, a mailing list or a ticketing system.

Future work: This procedure is quite stable, so no future developments are required. When new services require the usage of the EOSC hub helpdesk, this procedure will handle how to create their corresponding service units and the assignation of its responsibilities as service unit responsible.

3.12.3 Procedure ISRM3 How to assign role of 1st level support in the EOSC hub helpdesk service (xGUS)

This procedure defines the steps to assign a new person with the 1st level support role in the EOSC hub helpdesk. This procedure is required to be executed after the assignment of a new person in the 1st level support team of EOSC hub. The procedure is also linked to the User support guidelines document, which will need to be read and understood for the new 1st level support person.

There are no plans for further development of this procedure at present.

3.13 Problem Management (PM)

3.13.1 Procedure PM1 Periodic incident trend analysis

This procedure defines the periodic incident trend analysis required to detect recurrent problems. This analysis is done by checking all the incidents received in the EOSC hub helpdesk system. The review allows the process manager of PM to detect and generate the corresponding problem record to assign it to a problem owner. This review is done every 2 months and, as a result, it provides the problem records to include in the Known error database (KEDB).

The KEDB is implemented using the EOSC hub wiki. There is a specific page which contains a list of known problems detected in the periodic trend analysis. The status of each of the recurrent problems detected is reviewed in the Procedure 2, explained in the point 4.9.2.

Future work: Improve the analysis based on the previous expertise and improve the procedure to generate problem records and include them in the KEDB.

3.13.2 Procedure Review the KEDB content and keep up to date

This procedure defines the bi-annual review of the KEDB to ensure its completeness and correctness. The review removes possible duplicated problem records and reviews the status for each of the problems.

Future work: improve the review based on the expertise obtained from previous problem records, including new fields in the KEDB if needed or improving the Periodic incident trend analysis when required.

3.14 Continual Service Improvement (CSI)

The goal of Continual Service Improvement process is two-fold:

1. To identify, prioritize, plan, implement and review improvements to services and the service management system.
2. To manage the audit programme and management reviews, ensuring they are conducted and followed-up upon.

3.14.1 Policy Continual Service Improvement Policy

The purpose of Continual Service Improvement policy is to support the implementation of the overall service management policy, which specifically mentions continual improvement as an integral activity. The policy outlines that both EOSC hub services as well as the service management processes shall be continually improved. Feedback from stakeholders is to be used to continually improve EOSC hub services and service quality. All proposals for improvements are to be recorded and evaluated. EOSC hub service management is thus improved based on continual monitoring of process performance and effectiveness.

3.14.2 Procedure CSI1 Record, plan, coordinate and review all audits

This procedure describes the steps that need to be taken for managing audits (i.e. recording, planning, coordinating and reviewing audits).

Future work: The first of two internal SMS audits was conducted 11-15 March 2019. All aspects of the audit was documented in Confluence including roles, audit goals, classification of audit findings, audit plan/agenda, expected participants, full audit report, summary slides and an audio recording. Each audit findings have an individual JIRA ticket. The second audit has been agreed with the auditor and is provisionally scheduled for the first half of 2020.

3.14.3 Procedure CSI2 Identify, record, prioritise, evaluate and approve an opportunity and suggestions for improvement

This procedure describes the steps to identify, record, prioritize, evaluate and approve an opportunity / suggestions for improvement.

After the initial procedure was defined, an update was recently done to the workflow as a result of an improvement suggestion from the first internal audit. Future work includes better promoting the availability, objective and management procedure to increase usage.

3.14.4 Procedure CSI3 Manage and review the status and progress of improvements

This procedure describes the steps to manage and review the status and progress of all improvements.

Future work: This procedure was dependent on procedure 2 to be in operation. Now that this is in motion, this procedure can now be put into practice, which basically means to communicate its availability and purpose to relevant parties (i.e. Process Managers; Process Staff Members).

3.14.5 Procedure CSI4 Organise and conduct management reviews

Procedure describes how management reviews should be organised and conducted.

Future work: The first management review was held on 28 May 2019, which was scheduled as a follow-up to the first internal audit in order to evaluate the main audit findings and overall state of SMS implementation. A dedicated page and overall schedule is held in Confluence with actions in JIRA. During the first management review, it was decided to have an additional management review between the two audits, which is planned for Sept/Oct 2019. A third/final management review will be held immediately following the second/final internal audit scheduled for the first half 2020.

4 Conclusions

This deliverable has aimed to provide an overview of the aspects of the EOSC hub Service Management System have been developing with respect to the delivery of production services in the federated infrastructure. This has been done by providing an explanation of the fourteen processes, forty six procedures and six policies within the SMS at the time of writing this deliverable.

There have been many challenges of the work described within this deliverable, mainly as a result of the complexity of creating a new SMS from scratch, which largely consists of a federation of federations as well as including a wide range of different external services. At the same time it has proved challenging to interfacing this new SMS with already existing SMSes of the participating e-Infrastructures. For these reasons, this deliverable should be viewed as a snapshot of work that is very much still in progress and that will continue to develop during the remainder of the project. It is hoped that this work creates the foundations of the SMS of the EOSC that remains fit-for-purpose into the future.

5 References

This section contains links to all processes, policies and procedures mentioned in this document.

Identifier	*Description and Link*
SPM	Service Portfolio Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Service+Portfolio+Management+-+SPM
SPM1	Add a service in the EOSC Service Portfolio https://wiki.eosc-hub.eu/display/EOSC/SPM1+Add+a+service+in+the+EOSC+Service+Portfolio
SPM2	Change/retire a service in the EOSC Service Portfolio https://wiki.eosc-hub.eu/pages/viewpage.action?pageId=30739275
SPM3	Add or Retire a service in the Hub Service Portfolio https://wiki.eosc-hub.eu/display/EOSC/SPM3+Add+or+Retire+a+service+in+the+Hub+Service+Portfolio
SPM4	Modify a service in the Hub Service Portfolio https://wiki.eosc-hub.eu/display/EOSC/SPM4+Modify+a+service+in+the+Hub+Service+Portfolio
SLM	Service Level Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Service+Level+Management+-+SLM
SLM1	Negotiate, sign, update, resign the Hub service participation agreement https://wiki.eosc-hub.eu/display/EOSC/SLM1+Negotiate%2C+sign%2C+update%2C+resign+an+the+hub+service+participation+agreement+PA
SLM2	Negotiate, sign, update, resign the EOSC service participation agreement https://wiki.eosc-hub.eu/display/EOSC/SLM2+Negotiate%2C+sign%2C+update%2C+resign+an+the+EOSC-hub+service+participation+agreement+PA
SLM3	Manage EOSC service Participation agreement violation https://wiki.eosc-hub.eu/display/EOSC/SLM3+Manage+case+of+EOSC-hub+service+Participation+agreement+violation
SOCRM	Service Ordering and Customer Relationship Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Service+Order+and+Customer+Relationship+Management+-+SOCRM
SOCRM1	Service Order Management https://wiki.eosc-hub.eu/display/EOSC/SOCRM1+Service+Order+Management
SOCRM2	Responding to EOSC-hub 'Contact Us' requests https://wiki.eosc-hub.eu/display/EOSC/SOCRM2+Responding+to+EOSC-

	hub+%27Contact+Us%27+requests
SOCRM3	Recording and managing stakeholder information https://wiki.eosc-hub.eu/display/EOSC/SOCRM3+Recording+and+managing+stakeholder+information
SOCRM4	Provide technical support https://wiki.eosc-hub.eu/display/EOSC/SOCRM4+Provide+technical+support
SRM	Service Reporting Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Service+Reporting+Management+-+SRM
SRM1	Review a report catalog and reports distribution https://wiki.eosc-hub.eu/display/EOSC/SRM1+Review+a+report+catalog+and+reports+distribution
SRM2	Define, update, terminate a report https://wiki.eosc-hub.eu/display/EOSC/SRM2+Define%2C+update%2C+terminate+a+report
SRM3	Initiate follow-up actions in case of inaccurate reporting https://wiki.eosc-hub.eu/display/EOSC/SRM3+Initiate+follow-up+actions+in+case+of+inaccurate+reporting
SFRM	Supplier and Federation Member Relationship Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Supplier+and+Federation+Member+Relationship+Management+-+SFRM
SFRM1	Manage contractual disputes between the service provider and suppliers https://wiki.eosc-hub.eu/display/EOSC/SFRM1+Manage+contractual+disputes+between+the+service+provider+and+suppliers
SFRM2	Maintain the supplier and federation member database https://wiki.eosc-hub.eu/display/EOSC/SFRM2+Maintain+the+supplier+and+federation+member+database
CONFM	Configuration Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Configuration+Management+-+CONFM
CONFM1	Adding or removing a Configuration Item in the CMDB https://wiki.eosc-hub.eu/display/EOSC/CONFM1+Adding+or+removing+a+Configuration+Item+in+the+CMDB
CONFM2	Updating information in the CMDB https://wiki.eosc-hub.eu/display/EOSC/CONFM2+Updating+information+in+the+CMDB
CONFM3	Taking a Configuration Baseline before a new release https://wiki.eosc-

	hub.eu/display/EOSC/CONFM3+Taking+a+Configuration+Baseline+before+a+new+release
CONFM4	Verifying information stored in the CMDB on regular intervals https://wiki.eosc-hub.eu/display/EOSC/CONFM4+Verifying+information+stored+in+the+CMDB+on+regular+intervals
CHM	Change Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Change+Management+-+CHM
CHM Policy 1	Change Management Policy https://wiki.eosc-hub.eu/display/EOSC/Change+Management+Policy
CHM1	Open a Request for Change https://wiki.eosc-hub.eu/display/EOSC/CHM1+Open+a+Request+for+Change
CHM2	Define a Standard Change https://wiki.eosc-hub.eu/display/EOSC/CHM2+Define+a+Standard+Change
CHM3	Manage Emergency Changes https://wiki.eosc-hub.eu/display/EOSC/CHM3+Manage+Emergency+Changes
CHM4	Calculate the Risk Level https://wiki.eosc-hub.eu/display/EOSC/CHM4+Calculate+the+Risk+Level+of+a+Change
CHM5	Classify a change as Standard or Non-Standard https://wiki.eosc-hub.eu/display/EOSC/CHM5+Classify+a+change+as+Standard+or+Non-Standard
CHM6	Manage Standard Changes https://wiki.eosc-hub.eu/display/EOSC/CHM6+Manage+Standard+Changes
CHM7	Evaluate the risk level for Non-Standard Changes https://wiki.eosc-hub.eu/display/EOSC/CHM7+Evaluate+the+risk+level+for+Non-Standard+Changes
CHM8	Manage Normal Changes https://wiki.eosc-hub.eu/display/EOSC/CHM8+Manage+Normal+Changes
CHM9	Manage High-risk Changes https://wiki.eosc-hub.eu/display/EOSC/CHM9+Manage+High-risk+Changes
RDM	Release and Deployment Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Release+and+Deployment+Management+-+RDM
RDM Policy 1	Release and Deployment Management policy https://wiki.eosc-hub.eu/display/EOSC/Release+and+Deployment+Management+policy

RDM1	Internal Catalogue release and deployment process https://wiki.eosc-hub.eu/display/EOSC/RDM1+Internal+Catalogue+release+and+deployment+process
SACM	Service Availability and Continuity Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Service+Availability+and+Continuity+Management+-+SACM
SACM1	Manage an event of a major loss of service https://wiki.eosc-hub.eu/display/EOSC/SACM1+Manage+an+event+of+a+major+loss+of+service
SACM2	Create and maintain Service Availability and Continuity plans https://wiki.eosc-hub.eu/display/EOSC/SACM2+Create+and+maintain+Service+Availability+and+Continuity+plans
CAPM	Capacity Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Capacity+Management+-+CAPM
CAPM1	Create and Maintain a Capacity Plan https://wiki.eosc-hub.eu/display/EOSC/CAPM01+Create+and+Maintain+a+Capacity+Plan
CAPM3	Approve Capacity Plan https://wiki.eosc-hub.eu/display/EOSC/CAPM03+Approve+Capacity+Plan
ISM	Information Security Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Information+Security+Management+-+ISM
ISM Policy 1	EOSC-hub Security Policy https://wiki.eosc-hub.eu/pages/viewpage.action?pageId=34640606
ISM Policy 2	Acceptable Use Policy and Conditions of Use https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Security+Policy
ISM Policy 3	EOSC-hub Service Operations Security Policy https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Service+Operations+Security+Policy
ISM1	Security Incident Response procedure https://wiki.eosc-hub.eu/display/EOSC/ISM1+Security+Incident+Response
ISM2	Software Vulnerability Handling Procedure https://wiki.eosc-hub.eu/display/EOSC/ISM2+Software+Vulnerability+Handling+Procedure
ISM3	Information assets, threats, security risk assessments and controls https://wiki.eosc-hub.eu/display/EOSC/ISM3+Information+assets%2C+threats%2C+security+risk+assessments+and+

	security+controls
ISM4	Approval and adoption of ISM Policies https://wiki.eosc-hub.eu/display/EOSC/ISM4+Approval+and+adoption+of+ISM+Policies
ISRM	Incident and Service Request Management https://wiki.eosc-hub.eu/display/EOSC/Incident+and+Service+Request+Management+-+ISRM
ISRM1	How to handle incidents and service requests through the ticketing system https://wiki.eosc-hub.eu/display/EOSC/ISRM1+-+how+to+handle+the+Incidents+and+service+request+through+the+ticketing+system
ISRM2	Creation of a new service unit in the EOSC-hub helpdesk https://wiki.eosc-hub.eu/display/EOSC/ISRM2+Creation+of+a+new+service+unit+in+the+EOSC-hub+helpdesk
ISRM3	How to assign role of 1st level support in the EOSC-hub helpdesk service (xGUS) https://wiki.eosc-hub.eu/pages/viewpage.action?pageId=34639672
PM	Problem Management process homepage https://wiki.eosc-hub.eu/display/EOSC/Problem+Management+-+PM
PM1	Periodic incident trend analysis https://wiki.eosc-hub.eu/display/EOSC/PM+1+Periodic+incident+trend+analysis
PM2	Review the KEDB content and keep up to date https://wiki.eosc-hub.eu/display/EOSC/PM+2+Review+the+KEDB+content+and+keep+up+to+date
CSI	Continual Service Improvement process homepage https://wiki.eosc-hub.eu/display/EOSC/Continual+Service+Improvement+-+CSI
CSI Policy 1	Continual Service Improvement Policy https://wiki.eosc-hub.eu/display/EOSC/Continual+Service+Improvement+policy
CSI1	Record, plan, coordinate and review all audits https://wiki.eosc-hub.eu/display/EOSC/CSI1+Record%2C+plan%2C+coordinate+and+review+all+audits
CSI2	Identify, record, prioritise, evaluate and approve an opportunity and suggestions for improvement https://wiki.eosc-hub.eu/display/EOSC/CSI2+Identify%2C+record%2C+prioritise%2C+evaluate+and+approve+an+opportunity+and+suggestion+for+improvement
CSI3	Manage and review the status and progress of improvements https://wiki.eosc-

	hub.eu/display/EOSC/CSI3+Manage+and+review+the+status+and+progress+of+improvements
CSI4	Organise and conduct management reviews https://wiki.eosc-hub.eu/display/EOSC/CSI4+Organise+and+conduct+management+reviews