EOSC-hub

D4.2 Operational Infrastructure Roadmap

Lead Partner:	EGI Foundation
Version:	1.0
Status:	Final
Dissemination Level:	Public
Document Link:	https://documents.egi.eu/document/3422

Deliverable Abstract

In order to harmonize the operational procedures among a large variety of EOSC service providers, EOSC-hub uses and expands the existing federation services and policies of EGI and EUDAT, the main e-infrastructures involved in the project, to create the operational framework of the EOSC and bases its IT Management System on the FitSM standard. This implies that all the EOSC operational activities will be directed by policies and will be structured and organised by processes and procedures with the final aim to offer to the end users a single fluid platform ensuring the smooth interoperability of the various service offers. The document describes the consequent operations coordination work to harmonize activities and plans for service delivery among the involved actors, depicts the current status of implementation of the EOSC SMS and presents a roadmap to have it fully established and operational.

EOSC-HUB RE NDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT 6.

COPYRIGHT NOTICE

DELIVERY SLIP

Date	*Name*	*Partner/Activity*	*Date*
From:	Alessandro Paolini	EGI Foundation/WP4	2019-01-29
Moderated by:	Malgorzata Krakowian	EGI Foundation/WP1	
Reviewed by:	Nicolas Liampotis, Diego Scardaci	GRNET/WP5 EGI Foundation	2019-01-22, 2019-01-31
Approved by:	AMB		

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author(s)*
v. 0.1	2018-12-07	first draft, ready for external reviewers	Alessandro Paolini, Matthew Viljoen, Vincenzo Spinoso, Pavel Weber, Johannes Reetz, Giovanni Morelli, Isabella Bierenbaum, Joao Pina, David Vicente, Dave Kelsey
v. 0.2	2019-01-22	Added review comments	Nicolas Liampotis (GRNET)
v. 0.3	2019-01-29	Incorporated comments of first review	Alessandro Paolini
v. 0.4	2019-01-31	Added review comments	Diego Scardaci (EGI Foundation)
v. 1.0	2019-02-04	Final version	Alessandro Paolini

TERMINOLOGY

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

Terminology/Acronym	*Definition*
AAI	Authorization and Authentication Infrastructure
AppDB	Applications Database
AUP	Acceptable Use Policies
BDII	Berkeley Database Information Index
CA	Certification Authority
CAB	Change Advisory Board
CAPM	Capacity Management

CDI	Collaborative Data Infrastructure
CHM	Change Management
CMDB	Configuration Management Database
CONFM	Configuration Management
CRM	Customer Relationship Management
DPMT	Data Project Management Tool
EGI	European Grid Infrastructure
EOSC	European Open Science Cloud
EUDAT	European Data Infrastructure
FitSM	Free standards for lightweight IT Service Management
GDPR	EU General Data Protection Regulation
GGUS	Global Grid User Support
GOCDB	Grid Operations Configuration Management Database
IRTF	Incident Response Task Force
ISM	Information Security Management
ISRM	Incident and Service Request Management
ITMS	IT Management System
KEDB	Known Error Database
NGI	National Grid Initiative
OLA	Operational Level Agreement
OMB	Operations Management Board
OPCT	Operations Coordination Team
PM	Problem Management
RC	Resource Centre
RDM	Release and Deployment Management
RfCs	Requests for Changes
RP	Resource infrastructure Provider
SACM	Service Availability and Continuity Management
SFRM	Supplier and Federation Member Relationship Management
SLA	Service Level Agreement
SLM	Service Level Management
SMB	Service Management Board
SMS	Service Management System
SOCRM	Service Order and of Customer Relations Management
SP	Service Provider
SPF	Service Providers' Forum
SPM	Service Portfolio Management
TRL	Technology Readiness Level
UA	Underpinning Agreement
VO	Virtual Organisation

Contents

Executive summary

EGI and EUDAT are the main e-Infrastructures that provide federation, collaboration and common services as part of the EOSC-hub service catalogue. These services are complemented by Research Enabling/Thematic services offered by a number of mature Research Infrastructures (like CLARIN, WLGC, GEOSS, DARIAH, WeNMR, etc.) and other relevant initiatives. During the project lifetime, the initial service catalogue will be enriched with a variety of services and resources from other e-infrastructures, research infrastructures, research communities, projects, SMEs/Industry, etc. This large variety of providers has different experiences in service management and follows different policies and procedures for controlling and delivering their services. The goal of the WP4 is to harmonize the operational procedures among all these actors as much as necessary, according to the services integration level[1]: each provider decides to adopt and create the operational framework of the EOSC hub. In order to do so, EOSC-hub uses and expands the existing federation services and policies of EGI and EUDAT, the main actors of the project, and bases its IT Management System[2] on the FitSM standard[3]. This implies that all the operational activities will be directed by policies and will be structured and organised by processes and procedures with the final aim to offer to the end users a single fluid platform ensuring the smooth interoperability of the various service offers.

After an overview of the EGI and EUDAT operational frameworks, the current status of the harmonisation activities between these two frameworks is depicted with a focus on the operations coordination, the definition of the different levels of integration and the procedure to onboard new services and, then, expands the Hub. Two new operational boards were established: (1) the Service Provider Forum that aims to facilitate the communication between the Hub and the providers and enable the latter to influence the future direction of operational aspects of the EOSC Hub and EOSC in general; (2) the Service Management Board, a closed body intended solely for services with MEDIUM and HIGH levels of integration, with the additional aims of discussing problems involving operations, approval of changes to operational policies and to the on-boarding process.

Finally, current status of the EOSC SMS processes and the roadmap to finalise and make fully operative the EOSC SMS are depicted.

[1] https://documents.egi.eu/document/3342

[2] An IT service management system (ITSM) is the entirety of activities performed by service providers to plan, deliver, operate and control services offered to customers

[3] www.fitsm.eu

1 Introduction

The document describes the common operational framework that EOSC-hub project is developing, based on the FitSM standard, for controlling, operating and delivering the EOSC services. The deliverable is structured as follows.

Section 2 describes the EGI and EUDAT federations' operational framework: it will be presented as the basis for the establishment of the future EOSC operations. Section 3 depicts the federated activities of the EOSC ITSM focusing on the description of the on-going harmonisation work of policies and procedures of EGI and EUDAT e-infrastructures, introducing the new bodies Service Provider Forum and Service Management Board and describing the process for on-boarding and validating new services into the service catalogue. Furthermore, the current status of the implementation of the EOSC SMS processes is presented.

By comparing these two sections, it becomes evident the changes that the federations are going to deal with, and the continual improvement process they are going through. On one side, the EGI infrastructure, which is already implementing the FitSM standard and is certificated ISO 20000, will have to broaden its view considering new ways to operate and offer the services in the EOSC-hub environment with different providers, new services, and more different customers; on the other hand, the EUDAT federation will have to progressively adapt its operational framework to the FitSM requirements, procedures, and policies, starting a harmonisation process along the other participants of the project.

Before the conclusion, in section 4, it is presented a timeline of the activities that need to be completed in order to complete the implementation of the EOSC ITSM and to make it fully operative.

This document basically represents our vision on how the operational infrastructure will look like at the end of the project, describing all those activities that any member should carry on in order to deliver its services in according to the SMS requirements.

2 Status of the e-Infrastructures

In this chapter we briefly describe the main infrastructures participating in the project, EGI and EUDAT, with particular regard to the operations activities and the services that support them.

2.1 EGI Infrastructure overview

The EGI infrastructure[4] comprises resources provided across 47 countries. These resources are hosted, managed, and operated by the Resource Centres (RCs), the smallest resource administration domain in EGI (237, at the moment of writing). A RC can be either localised or geographically distributed: it provides a minimum set of local or remote IT Services compliant to well-defined IT capabilities (Compute, Storage, and Cloud) necessary to make resources accessible to the users by exposing common interfaces.

[4] https://www.egi.eu/

The Resource Centres (RCs) are federated in EGI through the affiliation to NGIs (National Grid Initiative), organisations set up to manage the resources provided in their countries by the RCs to the EGI Infrastructure. They represent the country's single point of contact for EGI as well as to liaise with government, research communities and resource centres as regards ICT services for e-Science.

Each NGI is supported by an Operations Centre, defined as a centre offering operations services on behalf of the NGI (or Resource infrastructure Provider (RP), more generally), and it can serve multiple RPs. EGI currently comprises 24 national Operations Centres and 7 federated Operations Centres supporting multiple NGIs.

In order to become a member of the EGI Infrastructure, each RC has to agree an Operational Level Agreement (OLA)[5]: it is an agreement between RPs and RCs for defining the provision and support of the provided services. In the document it is described the minimum set of Functional Capabilities (for example HTC computing, Cloud Computing, File Transfer and Storage Management) that a RC has to provide, besides some operational requirements in terms of quality of service provided (Availability/Reliability targets and average response time to the tickets).

2.1.1 Operations governance

The **Operations Management Board (OMB)**[6] is the EGI policy board that aims at defining policies needed to provide a reliable transparent infrastructure composed of multiple Operations Centres and Resource Centres. The OMB is made of representatives of the single NGIs (NOC Managers), of the technical services, and of the EGI.eu Operations Team. All the policies and procedure that are relevant to EGI Operations are collected centrally and available to the Operations Centres, Resource Centres and in general to the EGI Community. In particular, the EGI Wiki is used to share procedures on VOs[7] registration and decommissioning, RCs and OCs certification and suspension, support, monitoring and Availability/Reliability (A/R) metrics definition and reporting; on the other hand, the EGI Document Database is used for policies and reports, like SLA/OLA agreements and reports. Procedures let NOC managers to handle regional issues and foresee escalation to central EGI Operations whenever they fail.

The **EGI Operations meeting**, instead, is the place where technical discussions can happen about updates on upcoming software releases, operational issues, A/R reports, software deployment problems, news concerning tools deployed.

2.1.2 Supporting services

EGI Foundation and its partners provide for the member of the infrastructure a set of technical services and human activities, mostly operational, to enable the EGI federations and the daily provisioning of the services to EGI customers. For each of these services there is a dedicated OLA in place defining conditions under which the so-called “EGI Core Services” are offered to EGI Foundation by its partners. A brief overview of the Core Services more strictly related to operations activities is provided below.

[5] https://documents.egi.eu/document/31

[6] https://documents.egi.eu/document/117

[7] https://wiki.egi.eu/wiki/Glossary#Virtual_Organisation

Service Registry. GOCDB[8] is the Service Registry of EGI. It is used for the configuration management, namely to record information about different entities such as the Operations Centres, the Resource Centres, service endpoints and the contact information and roles of people responsible for operations at different levels. GOCDB is a source of information for several services in the infrastructure, like Monitoring, Accounting, etc., and the main source for site contacts, site information and configuration.

Monitoring. ARGO[9] is the monitoring service used in EGI to assess the working status of resources and services of the infrastructure, in according to the Service Level promised in the agreed OLAs. It includes remote monitoring of services, visualization of the their status, dashboard interfacing, notification system and generation of availability and reliability reports. Accordance with the procedures, the results of the probes are periodically collected to compute the monthly Availability and Reliability figures: these values are then the input for enforcing the RC OLA, notifying any violation to the agreed service level.

Operations Portal. The Operations Portal[10] is a central portal for the daily operations activities that offers a bundle of different capabilities, such as the broadcast tool, VO management facilities, resources discovery, a security dashboard for handling with security vulnerabilities occurring in the RCs, and an operations dashboard for handling with the failures detected by the monitoring service, allowing to open tickets to the affected Resource Centres thanks to the interface with the EGI Helpdesk system. The dashboard also supports the central oversight activities. It is a critical component as it is used by all EGI Operations Centres to provide support to the respective Resource Centres.

Accounting Repository and Portal. The Accounting Infrastructure (Portal[11] and Repository[12]) supports the daily operations of EGI and it is useful for assessing the real usage of the computing, cloud, and storage resources. It is a complex system that involves various sensors in different regions, all publishing data to a central repository. The data are processed, summarized and displayed in the accounting portal, which acts as a common interface to the different accounting record providers and presents a homogeneous view of the data gathered and a user-friendly access. There are dedicated views for NGI managers, VO Managers, RC administrators and the general public.

Helpdesk service and human support. The EGI Helpdesk service is based on the GGUS ticketing system[13], which is interfaced in a bidirectional way to the regional helpdesk systems used by several NGIs. GGUS is part of the EGI Collaboration Platform and is needed to support users and infrastructure operators. The support in EGI Helpdesk consists of three levels: the 1st support level is responsible for ticket triage and assignment and for the coordination with teams responsible for second and third support level. Software-related tickets that reach the second level of support are analysed and if necessary are forwarded to third line support units only when there are clear

[8] https://wiki.egi.eu/wiki/GOCDB

[9] https://wiki.egi.eu/wiki/ARGO

[10] https://wiki.egi.eu/wiki/Operations_Portal

[11] https://wiki.egi.eu/wiki/Accounting_Portal

[12] https://wiki.egi.eu/wiki/Accounting

[13] https://ggus.eu/

indications of a defect (in software, documentation, etc.). Recurring problems with related workarounds and solution are stored in a Known Error Database (KEDB). Monthly reports on support units' response time are produced in order to verify that the support activities have been provided in according to the service level defined in the several OLAs.

Security coordination and security tools. Central coordination of the security activities ensures that policies, operational security, and maintenance are compatible amongst all partners, providing monitoring services to check for security vulnerabilities and other security-related problems in the infrastructure: it guarantees that incidents are promptly and efficiently handled, that common policies are followed by providing services such as security monitoring, and by training and dissemination with the goal of improving the response to incidents. This includes liaison with external security organisations, coordination security training, of security service challenges and of security threat risk assessment.

Services for AAI. This activity is responsible of the **Check-in**[14] service, the AAI Platform for the EGI infrastructure that enables EGI users to collaborate, participate in groups and access resources and services in an intuitive, reliable and secure manner. The activity also supports a group management system (PERUN, for the access to cloud resources), the EGI Catch All CA and the VOMS Catch-All service.

2.2 EUDAT Collaborative Data Infrastructure overview

The EUDAT Collaborative Data Infrastructure[15] (CDI) is a network of currently 25 European research organisations across 14 countries, with the aim to support research communities and individual researchers by offering the services for storage, management, analysis and re-use of research data. The EUDAT CDI consists of several actors, while the main are service providers and customers. The service providers manage and deliver services to customers, working together under EUDAT CDI Agreement. According to the agreement any provider is classified either as generic or as thematic:

- Generic Service Providers have regional, organizational or national mandates to support scientific research, usually from different disciplines.
- Thematic Service Providers are discipline-specific organisations mandated to support a well-defined scientific community or group of customers and users.

The CDI agreement defines two provider levels according to the commitment:

- Level-1: generic or thematic services provider offers and operates the full stack of CDI B2 services and components; they ensure that provided B2 services are monitored and accounted; the local support line and security incident response contact are in place; the services are fully integrated in EUDAT SMS.

[14] https://wiki.egi.eu/wiki/AAI

[15] https://eudat.eu/

- Level-2: generic and thematic service providers offer one or a few B2 services, there is no requirement to provide the full stack of B2 Services; the provider ensures that provided services are monitored and accounted.

2.2.1 Operations Objectives

The operations in EUDAT CDI are governed by EUDAT Service Management Framework (SMF), which defines the policies and operational guidelines in federated environment. The main objectives of EUDAT operations coordination are:

- Consolidation of the operational environment of EUDAT CDI, ensuring the authenticity, integrity, confidentiality and preservation of data deposited by its users.
- Integration, commission and operation of the service components of the CDI throughout their lifecycle.
- Provisioning of storage resources and support of EUDAT data projects during enabling and production phases.
- Offering support to research communities and users in connecting their repositories to the CDI and using the EUDAT services.
- Ensuring the operational and infrastructure security of the EUDAT CDI, coordination of security activities e.g. regular security vulnerability scans.

2.2.2 Operations Organization

The main body of operations organization in EUDAT is the Operations Coordination Team (OPCT), which governs and performs the full set of operational tasks and duties. The core of OPCT consists of:

- Operations Coordination Team Leader.
- Deputies and representatives of generic and thematic providers.
- CDI security manager.
- CDI configuration manager.
- CDI change manager.
- CDI monitoring and accounting manager.

The OPCT conducts regular monthly meetings to address coordination of major changes, software upgrades, security related activities, integration of the new services and critical issues in the CDI infrastructure.

2.2.3 Operational Tools and SMS procedures

The core activities of OPCT are governed by application of a set of operational procedures which were developed in EUDAT according to the FitSM framework. These procedures are defined and described in EUDAT Service Management System (SMS).

In addition, several operational tools and services (the so-called “Internal Services”) are used together with procedures to perform the operations coordination. The main tools are:

- **JIRA** (Issue & Project Tracking Software) mainly used in change management. All change requests in EUDAT are created and tracked in JIRA according to the workflows defined in change management process definition.
- **DPMT** (Data Project Management Tool[16]) is a content management system for management and the implementation of data management plans during a managed enabling process. The tool registers service providers, services, service components, resources and data project requests. Mainly used for configuration management process and supplier relationship management.
- **SPMT**[17]: the Service Portfolio Management tool offers a database that allows service designers, developers and specialists to describe the planned or implemented features of the service portfolio. The EUDAT SPMT exports information about the mature CDI services and their service options to the Service Catalogue on the EUDAT website https://www.eudat.eu/catalogue. This catalogue renders the service descriptions for external consumption.
- **RT** (Request Tracker[18]) is a helpdesk system which delivers the first-level support and also second and third levels in incident and service request management process implemented in EUDAT. The incident tickets if not solved at first-level support are distributed to the corresponding support teams of the EUDAT services for further processing and resolution.
- **SVMON**[19] (Software Monitoring Framework) collects information about the installed software versions of services and components in the EUDAT CDI and facilitates the configuration management. The SVMON is also used to control and coordinate major changes in the infrastructure which affect multiple core EUDAT services.
- **ARGO**[20] Monitoring system was adopted by EUDAT for executing functionality tests on the (distributed) service instances that are registered in the DPMT and produces availability/reliability reports.
- **ACCT**[21] is EUDAT accounting repository that stores accounting data on allocated, pledged and used storage within the EUDAT CDI, providing an API for registered accounting clients to upload usage records associated with the service instances.

- **B2ACCESS** service[22]: a proxy AAI service is being operated in combination with an instance for the integration of new services and with a staging instance for testing software components before the service and software is being released and updated. Used by most of the EUDAT services, B2ACCESS is one of the critical components of the CDI.

[16] https://dp.eudat.eu

[17] https://sp.eudat.eu

[18] https://helpdesk.eudat.eu

[19] https://svmon.eudat.eu

[20] https://avail.eudat.eu

[21] https://accounting.eudat.eu

[22] https://b2access.eudat.eu

3 Operating framework of the EOSC-hub infrastructure

Integration within EOSC aims to achieve a level of interoperability between services and processes in the participating infrastructures and the service providers to offer to the end users a single fluid platform governed by processes which ensure the smooth interoperability of the various service offers.

3.1 Harmonization work

The first activity at the beginning of the project within Task 4.1 Operations Coordination was the identification of the areas where the harmonization activities could initially focus across the participating key e-Infrastructures (EGI and EUDAT) in the project. These areas were agreed to be the following:

- Operations governance: it was recognised from an early stage that when services are delivered through EOSC-hub and are operated within a common Service Management System, there needs to be some form of governance covering all aspects of the service delivery. This would act as a link between the organisations running the service and the management of the project. It was agreed that this may be fulfilled by means of a Service Providers Board, described in more detail in Section 3.3.

- Monitoring: as fundamental tool to guarantee the quality of the services offered through the Hub. Since both participating key e-Infrastructures in the project make use of ARGO as monitoring service, it seemed logical to look at the current ways that monitoring was being done and move towards a common approach, both in terms of the probes themselves as well as the procedures surrounding them. At the time of writing this deliverable, this is an ongoing activity.

- Resource centre registration and certification: harmonization will be achieved with a new procedure l for registering new RCs in the Hub, keeping into account the need of negotiating an OLA with the RCs willing to join the EOSC, the information that has to be stored in the configuration database, the security aspects, and the requirements for certifying in production a RC. EGI and EUDAT will maintain a certain autonomy in managing their RCs, but most of the procedures and the policies (e.g. the security ones) will be the same.

3.2 On-boarding and validation of new services into the service catalogue

Service on-boarding within EOSC-hub is the process whereby a new service joins the EOSC service catalogue and EOSC Marketplace. This provides services with all the benefits offered by the Hub: promotion of the service to users outside their local community domain, a single gateway for users to discover and use services, regardless of their nature and their scientific domain, and potential integration with other services in the catalogue.

The operational requirements for joining the catalogue from the Service Management System (SMS) are defined in deliverable D4.1 “Operational requirements for the services in the catalogue”[23], structured around different operational parts of the SMS covering the service delivery. However, the on-boarding process itself is not covered in D4.1. This section aims at outlining this basic workflow, which is accurate at the time of writing this deliverable. The onboarding procedure will be further evolved according to the experience that will be gained in the next months and further changes will be made in subsequent versions of this deliverable.

3.2.1 Service Catalogues and Levels of Integration

The on-boarding process is based on the basic ideas first expounded in D4.1, which are briefly summarized here for the benefit of the reader. These concepts are fully explained in D4.1 “Operational requirements for the services in the catalogue”.

Within EOSC-hub there are two service catalogues:

1. the internal catalogue containing access-enabling services developed as part of the project and necessary for the operation of the EOSC hub (e.g. helpdesk and AAI);
2. the external catalogue containing research enabling services that are further classified in common services, which are generic services on which other services can depend (data, compute, orchestrators), and thematic services, offering scientific facilities to the end user, typically building on the common services.

Alongside these two services catalogues, services may attain three levels of service integration:

1. **LOW** level has the minimum set of SMS requirements. Nevertheless, along with all other services in the external catalogue, services entering at this level benefit from the advantages of the EOSC-hub as listed above. Services which enter the catalogue at this level may either have a less mature SMS which they plan to develop, or a mature SMS but would like to join the EOSC-hub initially without committing additional resources for integration until a later stage.
2. **MEDIUM** level is aimed at services in the external catalogue that are being delivered as part of an existing and mature SMS complying with the majority of requirements of FitSM or other recognised Service Management Framework. Services achieving a Medium level of integration are encouraged to participate closely with the EOSC-hub by being represented at the Service Management Board meetings.
3. **HIGH** level is for services in the internal catalogue delivered as part of the EOSC-hub SMS. Services from the external catalogue may also achieve this highest level of integration. Services with a High level of integration are expected to participate closely with the EOSC-hub and expected to be represented at the Service Management Board meetings.

[23] https://documents.egi.eu/document/3342

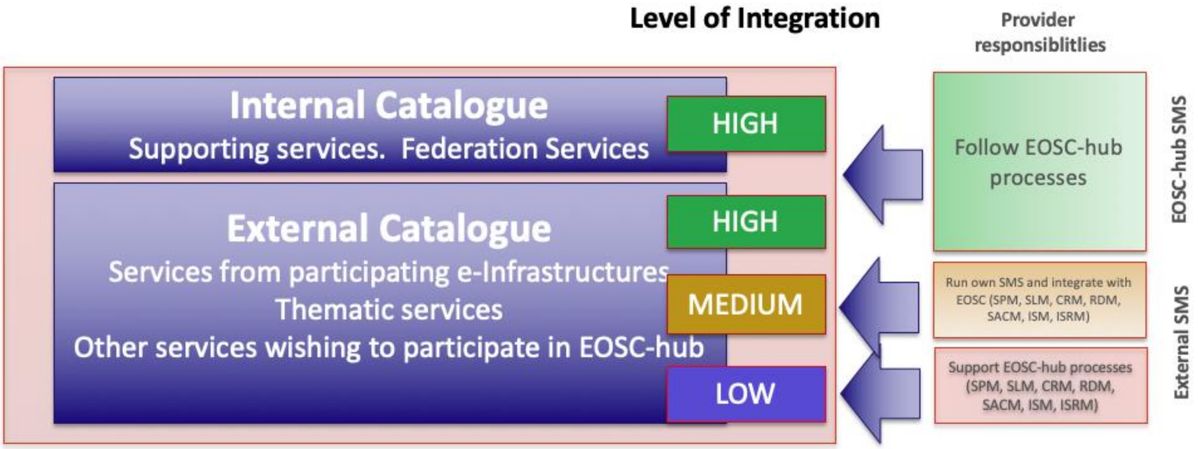
Level of Integration
Provider responsiblitlies
Internal Catalogue
Supporting services. Federation Services
HIGH
External Catalogue
Services from participating e-Infrastructures
Thematic services
Other services wishing to participate in EOSC-hub
HIGH
MEDIUM
LOW
Follow EOSC-hub processes
Run own SMS and integrate with EOSC (SPM, SLM, CRM, RDM, SACM, ISM, ISRM)
Support EOSC-hub processes (SPM, SLM, CRM, RDM, SACM, ISM, ISRM)
EOSC-hub SMS
External SMS

Figure 1 - The diagram above shows how the two Service Catalogues and three levels of integration work together. The acronyms mentioned in the diagram are taken from FitSM.

It is anticipated that new services wishing to join the EOSC-hub service catalogue will be probably joining the External Catalogue at the LOW level of integration, and if they wish, move to MEDIUM or HIGH at a later date. EOSC-hub will encourage providers to move to higher levels of integration and will assist Service Providers during this process. However, the on-boarding process for each level is similar and is described in the next section below.

3.2.2 On-boarding Process

This section outlines the basic process for on-boarding, which is illustrated in Figure 2.

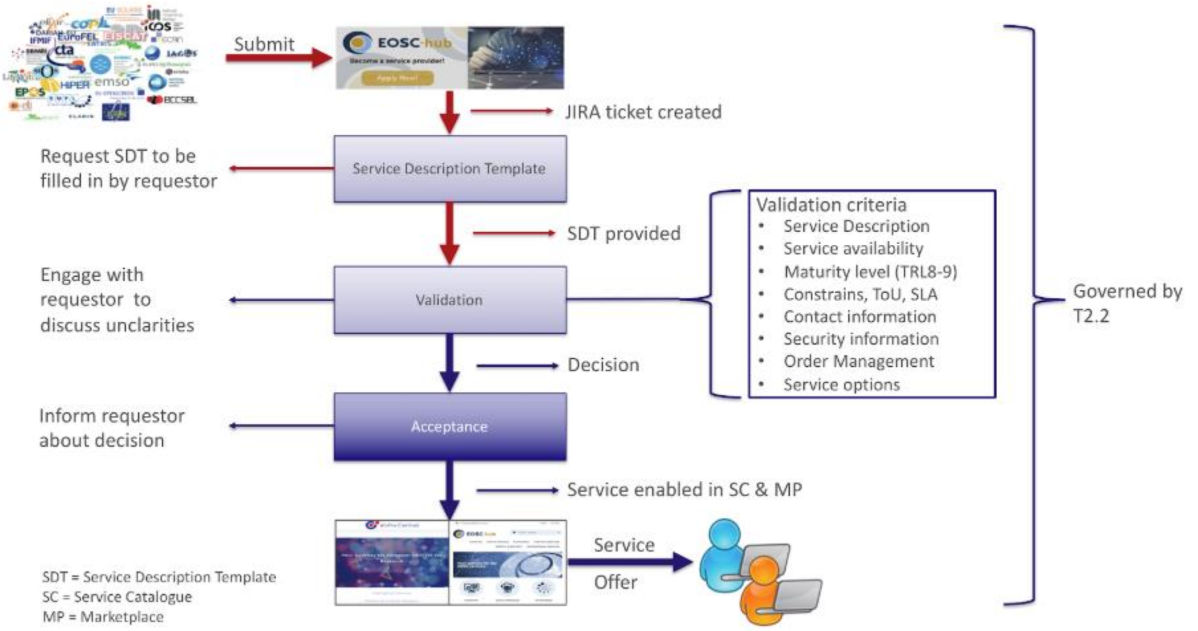

Figure 2 - The basic on-boarding process for new service providers in EOSC-hub.

1. *Initial contact is made with EOSC-hub by the prospective service provider*: the prospective Service Provider completes the “Join as a provider” form on the EOSC Portal, providing high-

level information about the service and motivation for joining. The submitted information becomes a ticket in the EOSC-hub issue tracking tool[24] to track the request.

2. *Initial evaluation of request*: EOSC-hub staff working with Service Portfolio Management (EOSC-hub Task 2.2) evaluates the request, contacting the submitter for supplementary information to initially gauge the high-level validity of the request and to confirm that the service is appropriate for inclusion into the service catalogue. If so, the prospective service provider fills in the Service Portfolio Entry Template (at least all mandatory fields) and Service Options are discussed.
3. *Determination of the initial level of integration and Verification of requirements*: EOSC-hub staff working with Operations Coordination (EOSC-hub Task 4.1) review the operations validation checklist to evaluate the maturity of the service (i.e. TRL level of at least 8 - see Appendix I) and the maturity of the SMS of the Service Provider. This may be done as an online meeting with the service provider, and the checklist may be sent in advance to aid preparation for the meeting. The initial level of integration is agreed with the Service Provider.
4. *EOSC-hub SMS Process Integration*: at this point where all requirements are fulfilled at the agreed level of integration, the following steps are required. All the progresses are tracked in Jira.
    a. *Adding the new service to the catalogue (EOSC-hub Task 2.2):* Information required by SPM about the service is added to the catalogue by creating an entry in the EOSC-hub SPMT instance[25].
    b. *Preparation for SLA creation (EOSC-hub Task 4.2)*: the SLA template is populated for the new service in readiness for SLAs with end users, and the service contact is made familiar with its format.
    c. *Security (EOSC-hub Tasks 4.4, 4.6)*: the nominated contact from the Service Provider (or another nominated security contact) is added to the appropriate database (e.g. GOCDB) for security-related issues.
    d. *Support (EOSC-hub Task 4.5)*: for services at a LOW and MEDIUM integration level, the appropriate contact for providing support is added to the EOSC-hub catalogue. For services at a HIGH integration level, a new support unit is created in XGUS and associated with the appropriate contact for providing support.
    e. *Marketplace integration (EOSC-hub Task 5.2)*: the prospective Service Provider completes the Marketplace Service Description Template providing information relevant to the Marketplace. Other existing services on the marketplace are introduced that may be relevant and of interest for potential future integration.
    f. *Operational integration (EOSC-hub Task 4.1)*: a nominated contact from the Service Provider is invited to engage with the Service Provider Forum by joining its mailing list and attending quarterly meetings. The Service Provider Forum is designed to facilitate communication between Service Providers and the EOSC Hub, in addition to requirements gathering. If the level of integration is MEDIUM, the nominated

[24] https://jira.eosc-hub.eu/

[25] https://eosc.agora.grnet.gr/

contact from the Service Provider is additionally invited to attend Service Management Board meetings.

3.3 Service Providers' Forum (SPF) and Service Management Board (SMB)

A fundamental aspect of successful coordination of service delivery is communication between the Hub and the service providers. The primary aim of the Service Providers' Forum (SPF) is to facilitate such communication in both directions:

1. **Communication from the Hub to Service Providers:**
    a. Status and news, including EOSC news, major operational news, security threats and upcoming events.
    b. Increasing the awareness of access enabling services: how new services may benefit from access enabling services; methods of integration and the provision of new access enabling services.
2. **Communication from the Service Providers to the Hub**
    a. Requirements collection covering the needs of Service Providers and how EOSC may facilitate their work in an evolving environment.
    b. Feedback to the Hub from not only the Service Providers themselves, but also **from their users**. It is often challenging for federations of services to gather feedback from large user bases, however the Service Providers is one important channel that may be exploited.

It is hoped that the above points become an important factor of Service Providers joining the EOSC Hub and serving the needs of their users, even at the lowest level of integration. This may be facilitated by open communication channels for the SPF such as a mailing list, virtual meetings where all SPs are invited to attend in addition to F2F meetings at EOSC-hub conferences. Membership of the SPF is open to anyone; however it is recommended that e-Infrastructures may be represented collectively to address scalability issues.

However, there needs to be added value for SPs to want to achieve higher levels of integration, and we believe that the means to help achieve this is by providing SPs with greater influence in shaping the future direction of operational aspects of EOSC-hub and EOSC in general. For this reason, the SPF is not sufficient in itself - a higher level body is required with management aspects. This body is the **Service Management Board (SMB)**, a closed body intended solely for services with MEDIUM and HIGH levels of integration. This body addresses the same communication aims as described above, with the additional aims being:

- Discussion of problems involving operations and possible solutions.
- Discussion and approval of /non-strategic/ changes to operational policies.
- The on-boarding process and changes to it.

As with the SPF, the SMB is planned to meet by virtual meetings on a needs-be basis, with ongoing communication facilitated by a closed mailing list, with membership for people representing services with a MEDIUM and HIGH levels of integration and e-Infrastructures collectively represented. The body is planned to report to the project Activity Management Board (AMB), with any strategic changes being deferred to the AMB.

3.4 Federated activities - SMS processes

In this section, we describe the activities that represent the “core” of the operational infrastructure, with each FitSM process taking care of some aspects of it, and the work done since the beginning of the project to set it up.

3.4.1 Service Level Management

The process contributes to maintain a service catalogue and define, agree and monitor service levels with customers by establishing meaningful service level agreements (SLAs) and supportive operational level agreements (OLAs) and underpinning agreements (UAs) with providers. It interfaces to CAPM, SACM, and SOCRM processes for defining the requirements in the several agreements concerning customers’ feedback or service capacity, availability, and continuity aspects; the interface with SFMRM process, which monitors the performance of suppliers and federation members, ensures that the agreements are enforced.

The initial work has been focused in defining an OLA template for the EUDAT services, aiming to close the gap between EGI and EUDAT in this area: the ultimate goal is providing a harmonised OLA for all the EOSC service providers.

3.4.2 Supplier and Federation Member Relationship Management

The purpose of Supplier and Federation Member Relationship Management (SFRM) is to identify suppliers and federation members; ensure that there is a designated contact responsible for managing the relationship and communication with the supplier and federation member, and monitoring the performance of suppliers and federation members.

Following a series of scoping discussions that took place during the first year of the project, we have agreed that the Service Providers within EOSC-hub federation are the federation members rather than the suppliers of services, so we do not, at present, expect there to be any ‘suppliers’ of services in EOSC-hub. Furthermore, it is up to the federation members to manage agreements with their suppliers in the form of OLAs. Although delegation of this task can be requested by the EOSC-hub SMS, the activity itself is out of scope of the EOSC-hub SMS. For this reason, the SFRM process is presently confined to keeping track of the federation members, which are the e-Infrastructures within the project including any other Service Providers that achieve the HIGH level of integration.

Apart from the scoping discussions, activities so far within SFRM included setting up the SFRM database and starting populating the database with the existing federation members along with the contact details.

3.4.3 Order and Customer Relationship Management

The purpose of the Order and of Customer Relations Management (SOCRM) is to propose, share and approve the entire workflow related to the management of orders and the customer. To aid the reader in understanding the proposed procedures, we need to provide clarifications on the following aspects:

1. Origin of orders
2. Macro types of orders
3. Resources involved in the process and orders life cycle

1. Origin of orders

Regarding the origin from which the orders come, we must distinguish between the phase prior to the release in production of the marketplace to that in which the same came into production. Until the marketplace enters production, the order source is represented by the request form displayed by the EOSC web portal at the URL:
https://www.eosc-hub.eu/order-service.
Vice versa, in production, all orders will be collected from the marketplace at the following URL:
https://marketplace.eosc-portal.eu.
Task 4.2 helped to develop a model for managing orders in both scenarios.

2. Macro types of orders

The orders are in fact the requests sent to EOSC: these can mainly be of two types:

- Requests for services to be used by customers
- Service Providers offers of services to be displayed in the EOSC catalogue

It is obvious that the nature of these requests (active and passive in relation to services) is of a different nature: the goal of Task 4.2 is to propose a workflow model that "harmonises" the flows and makes use of the same architectural solutions, where possible.

3. Resources involved in the process and orders life cycle

In order to have a clear picture of the actors involved in the process and therefore of the resources, we have to discuss, as in point 1, the two different scenarios: *before and after the entry into production of the marketplace*. In relation to the first phase, we can refer to the Figure 3:

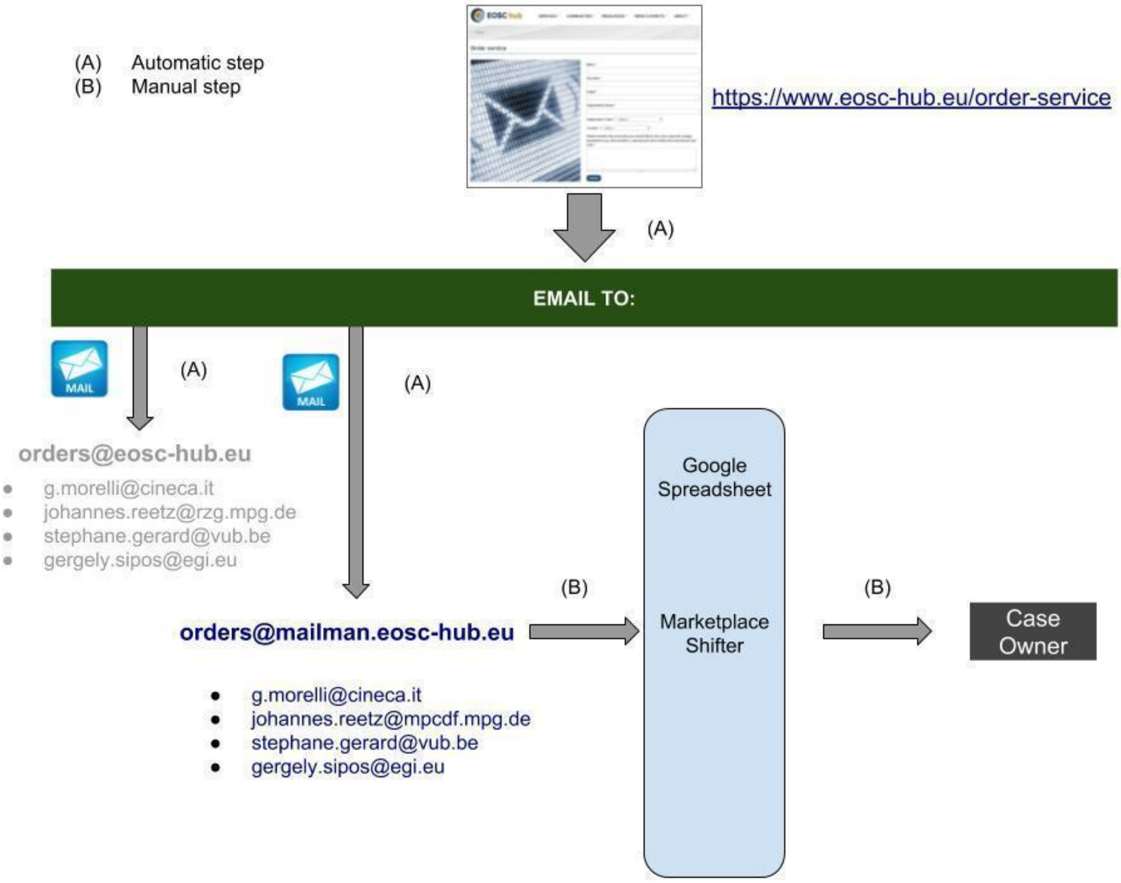

Figure 3 - Main actors in the service orders workflow before the Marketplace "in production" status.

The main actors in this workflow are:

- The EOSC portal
- The mailing lists
- The Marketplace shifter
- The Case Owner

Through the form on the EOSC web portal, the user fills in a form and generates an email message at the time of submission. All the steps described up to this point are automatic and are based on sending emails. Once the notification message is retrieved, the *Marketplace shifter* takes care of the request and intervenes "manually" in all the subsequent phases of the process. This role is central both in the current workflow and in the production one based on the marketplace: it is a resource of Task 4.2 that is allocated through an internally agreed rotation. The main actions of the Marketplace Shifter in this context are:

- Updating a shared document to track the status of orders and other information
- The identification of a Case Owner who takes responsibility for fulfilling the order

It is clear that this workflow has certain constraints, such as the need for manual interventions and the use of "one-way" notification mechanisms that do not allow automatic synchronization of notifications on actions carried out for a given order. However, the realization of this procedure was necessary in order not to disperse the orders during the transition to the Marketplace: the experience gained from this workflow has allowed us to design a new flow based on the Marketplace, as illustrated in Figure 4.

The new workflow has the following advantages over the previous approach:

- Most flows are managed automatically
- The central role assumed by Jira
- The ability to manage requests with "local" tools

As in the previous workflow, based on sending emails to the mailing list, also in this case a fundamental role is played by the Marketplace Shifter, which in this context works exclusively on the Jira platform: its activity in this case is semi-automatic in the sense that some requests (issue, in the Jira language) can be automatically forwarded to a specific peripheral management system (RT, DPMT, ..., Community specific system) while in other cases, less clear and more specific, they must be managed manually.

An important aspect of this workflow is that related to the synchronization of order management activities: in practice it is a matter of centrally managing an order that, by its nature, could be distributed over several centres to be processed. In this situation, each peripheral centre has its own ticketing system[26] through which to handle requests. This allows local operators to manage internally (EUDAT, EGI, Thematic centre ...) requests and to update their status on Jira in a "transparent" way through API synchronization. In this way at any time it is possible to look to a service request from a single point of consultation (Jira, in this schema) and obtain information on its progress.

In this first phase the work of Task 4.2 concentrated above all on the construction of a workflow for the management of orders in the different scenarios (in particular before and after the release of the Marketplace): as regards the Customer Relationship Management (CRM), the main activity was setting up a service satisfaction survey form of the services offered by EGI and EUDAT.

Among the next activities of Task 4.2 is the harmonization of these surveys starting from a shared template for all the services in the EOSC catalogue.

[26] EUDAT, for example, has an instance of RT that answers the address http://helpdesk.eudat.eu

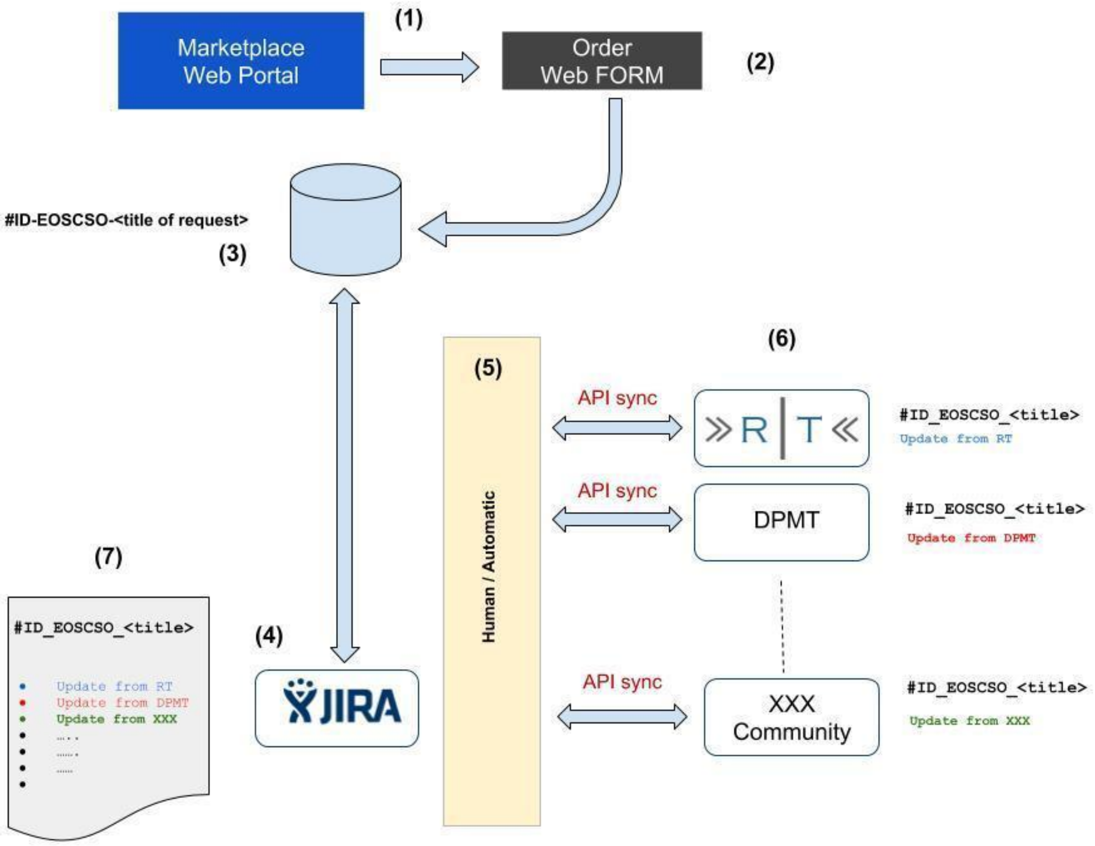

Figure 4 - Orders workflow: from creation to updating.

3.4.4 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 OLA and the availability needs in general, and that an adequate level of service continuity is guaranteed in case of exceptional events. The process makes sure of properly monitoring the services availability in order to detect a failure as soon as an incident occurs and then to trigger the ISRM and the PM processes for reporting the incident and for working on its resolution. The monitoring framework used by EOSC-hub will allow to:

- Monitor the services and their components after the registration in the CMDB (see Section 3.4.8);
- Execute specific probes periodically at configurable intervals in order to monitor the status of the services by emulating what the user can perform on them;
- Easily add new availability and reliability metrics, apply changes to the existing ones, remove the old ones;
- Produce customisable availability and reliability reports based on the monitoring data.

SACM is also responsible for minimising the risk of incidents: the conduction of risk assessment and management exercises aims to reduce risks to services to agreed acceptable levels and to plan and prepare for their recovery. As outcome, a Service Availability and Continuity Plan is produced, covering the definition and planning of the measures needed to be implemented in order to reduce the probability and the impact of the identified availability and continuity risks. In the plan it is also included an availability and continuity test to verify the robustness of the adopted measures and of the service recovery procedures.

Moreover, the process identifies new Availability and Continuity requirements and proposes changes to the existing ones based on several sources, like for example the services availability history, customer satisfaction and complaints, services reviews: changes to the requirements will then trigger the OLA's re-negotiation and Service Availability and Continuity Plans reviews.

3.4.5 Capacity Management

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. Capacity Management (CAPM) is usually triggered before the release of a service into the production environment (during the production of SDTP), with a periodic reiteration during all the lifetime of the services in the catalogue: the process considers all resources required to deliver the IT service, and plans for short-, medium-, and long-term business, capacity, and performance requirements. The result of this analysis is the production of 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. The plan clearly specifies any assumptions made as well as any recommendations quantified in terms of resources required, cost, benefits, impact, etc.

3.4.6 Information Security Management

The goal of this process is to manage information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information assets are preserved. The process will define security policies and procedures which will complement the security best practices implemented by the individual service providers. These will include operational and incident response policies, participant responsibilities, traceability, legal aspects, and the protection of personal data. The policies and procedures will not interfere with the local security best practices implemented by the individual service providers, but will build on them to ensure collaboration and uniform interoperations between service providers.
The process will coordinate an incident response task force (IRTF) to make sure that routine issues and security events are handled properly, and to provide specialised expertise in forensics and coordination for large scale incidents that threaten multiple providers. The process will also handle software vulnerabilities with the purpose to minimise the risk to the services and the users. Trust and interoperability will be promoted with other federated e-Infrastructures, Research

Infrastructures, and GÉANT via, for example, the activities of international initiatives such as the WISE Community[27].

3.4.7 Incident and Service Request Management, Problem Management

Incident and Service Request Management (ISRM) is the process responsible for restoring normal / agreed service operation within the agreed time after the occurrence of an incident, and for responding to user service requests. The goal of the Problem Management (PM) process is to minimize the number and the severity of the incidents/problems, and to prevent recurrent incidents. The ISRM and PM processes require to store, categorize and prioritize the requests received from the users, taking into account the SLAs of each service. The use of a ticketing system is highly recommended to manage these requirements and also to be able to escalate, resolve the issues and to keep the end user aware of the issue's progress. In EOSC-hub, the main ticketing system is xGUS. This service will act as the main contact point for the EOSC-hub service users to send their requests or incidents. Given that there are multiple e-infrastructures providing services through EOSC-hub, xGUS will need to be integrated with the ticketing systems of the participating e-infrastructures, i.e. EGI and EUDAT.

The Problem Management process requires the definition of a Known Error Database (KEDB), in order to store all the known errors records. The plan is to use the xGUS ticketing system for managing the Error Database. To achieve this, the required fields for the KEDB will need to be added to xGUS.

3.4.8 Configuration Management

The Configuration Management of the EOSC-hub (CONFM) has been created to provide and maintain a logical model of all configuration items (CIs) and their relationships and dependencies. It forms the basis and central point of information provision for all processes of the EOSC-hub that need to obtain, store, or update information on Configuration Items. This includes interaction with the Change Management (CHM), the Problem Management (PM), Incident and Service Request Management (ISRM), as well as the Service Availability and Capacity Management (SACM). The most important feature of the CONFM is the Configuration Management Database (CMDB). The CMDB of EOSC-hub is a distributed CMDB, currently consisting of GOCDB and DPMT, which stores the relevant information on Configuration Items necessary to run the Services that fall under the control of the EOSC-hub Configuration Management. Since the EOSC-hub CMDB is a distributed DB, the same procedures for the Configuration Management in the respective Service Management System have to be followed. Software versions in all CMDB are automatically checked and centrally provided by the service version monitoring software SVMON.

3.4.9 Change Management

The goal of the EOSC-hub Change Management (CHM) is to ensure that changes to Configuration Items (CIs) are planned, approved, implemented and reviewed in a controlled manner, such that negative impact of changes to services and ultimately to customers can be avoided. Possible changes could be updates of service versions, but also a changed contact person. The CHM plays an

[27] https://wise-community.org/

important role in the federated environment, where changes on CIs could affect other federation members, which might not be foreseeable by the person requesting the change.

The process provides procedures for three types of changes: Emergency Changes, Standard Changes and Non-standard Changes. Emergency Changes are changes that need an immediate action, like, for example, software updates to fix security threats. Standard Changes are evaluated once for their risk and impact on the Service Management System (SMS), and, if approved, added to the List of Standard Changes, such that they are pre-approved in subsequent occasions. The remaining changes are Non-standard Changes, which are assessed by a Change Management procedure to be of low or high risk. High-risk changes can only be approved through the Change Advisory Board (CAB). The CAB is a board which consists of senior project members and, if necessary, external experts able to make decisions on requested changes. It is called by the Change Manager to review and decide on any problem related to the CHM process, including but not limited to the review process after Emergency Changes and the decision to mark a change as a Standard Change.

The Change Management is not directly accessible from the outside, but is sheltered from external requests by other processes. However, Requests for Changes (RfCs) can in principle be raised by anybody inside the EOSC-hub SMS. Quite naturally, the Change Management in this sense interacts with the Incident and Service Request Management (ISRM) and Problem Management (PM), but also for example with the Information Security Management (ISM) and Continuous Service Improvement (CSI). On the other hand, the Change Management exchanges information like scheduled changes, planned and deployed releases, information on Configuration Items, as well as Change Records with the Release and Deployment Management (RDM) and the Configuration Management (CONFM). There also exists the possibility to interact with the Service Portfolio Management (SPM) in case of the addition, removal or status change of services. More generally, the various steps in the Change Management workflows imply discussions and interaction with various parties, ranging from the change requester and the service owners of affected services to anybody in the SMS whose involvement and feedback is necessary to estimate the consequences and risks of a change.

All RfCs are raised by opening a JIRA ticket in the EOSC-hub CHM JIRA project. This ticket contains fields that collect information about the requested change, like, e.g., the type of change, the expected duration, the risk level, the effect on other EOSC-hub services etc.. The life-cycle of the ticket implements the CHM workflow: Sending the ticket triggers an email to the Change Management process, which informs about the creation of a new ticket. The latter will then be processed according to its type and risk evaluation. Tickets are stored in a corresponding JIRA dashboard to follow and manage the various steps in the workflow, as well as for archiving reasons.

3.4.10 Release and Deployment Management

The goal of Release and Deployment Management (RDM) 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. This policy should identify different type of release such as major, minor and emergency within a predefined schedule.

So, all changes to IT resources, services and / or systems approved by the EOSC-hub Change Management are required to follow this Release policy. 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.

4 Plans for fully implementing the operational infrastructure

In this chapter we provide a plan until the end of the project to have the EOSC hub IT Management System fully implemented.

4.1 Supplier and Federation Member Relationship Management

As mentioned in Section 3.4.2, the bulk of this process is delegated to federation members within the EOSC hub since there are no suppliers of services within the project itself. Due to this fact, the focus of the remaining work in this process will be put on ensuring that the delegated activity happens in a satisfactory manner and that the relationship between the Hub and the federation members remains optimal. This is especially the case if more services reach the HIGH level of service integration.

4.2 Service Level Management

After defining the templates for SLAs, OLAs, and UAs, some effort is going to be spent for identifying the most important services in the catalogue needing an agreement to be in place and for the negotiation with the relevant service providers (for the cases not already handled by EGI and EUDAT). The following table provides a timeline for the actions that we plan to complete:

Table 1 SLM plan.

Action	***Target date***
Corporate SLA is in place	Dec 2018
Define SLAs, OLAs, and UAs templates	Jan 2019
Identify the most critical supporting service components, and agree OLAs and UAs with those contributing to delivering services to customers.	Q1 2019
Agree individual SLAs with customers for the most important / critical services.	Q1 2019

4.3 Service Order and Customer Relationship Management

The plan for the coming months includes completing the Customer Database, finalising the procedures and testing the process “*a regime*”.

Table 2 SOCRM plan

Action	***Target date***
Finalise the procedures	Jan 2019
Define templates for orders, complains, and service reviews	Jan 2019
Complete the Customers DB and testing the process "*a regime*"	1st half 2019

4.4 Service Availability and Continuity Management

The monitoring data currently available are the ones provided by the monitoring instances run separately by the e-Infrastructures: the ARGO Service Level Monitoring framework is adding support for multi tenancy that will simplify the creation of new Availability and Reliability or Status reports covering the already existing EGI and EUDAT services, the new ones that will be jointly provided, and services from other providers willing to join the EOSC Hub federation.

In the following table there is a list of actions that we plan to complete in the coming months in order to fully implement the process:

Table 3 SACM plan

Action	***Target date***
Finalisation of the procedures	Dec 2018
Collecting Availability and Reliability Metric data for the services registered in the EOSC-hub CMDB	Jan 2019

4.5 Capacity Management

Several services in the catalogue are offered by EOSC via the federation members, who are the ones having full control of the resources, also in terms of funding (e.g. Computing, Cloud, and Storage resources). Other services are provided by the federation members on behalf of EOSC-hub (e.g. the services in the internal catalogue[28]) that has more power decision on them. So it is crucial to define the scope of the process and of the procedures: for which services it is required a capacity plan, which parameters need to be taken into account, and for which services the process provides only suggestions in terms of capacity, leaving any decision to the providers. In the case of services like Computing, Cloud, and Storage, the information about the resources capacity and consumption is made available in both the Information System and the accounting services. For other services in the

[28] https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+service+catalogue

catalogue, we might need to make the information available only to the providers of the services, for example obtainable only through telemetry.

In the following table there is a list of actions that we plan to complete in the coming months in order to fully implement the process:

Table 4 CAPM plan

Action	***Target date***
Definition of the scope	Dec 2018
Finalisation of the procedures	Dec 2018
Define the structure and format of a (generic) capacity plan	Jan 2019
Define an approach to monitor service performance and capacity (including utilisation of resources) to record the results on an ongoing basis	March 2019

4.6 Information Security Management

In PY2 and PY3, the ISM process and its related policies and procedures will be updated as required. The complete plan is provided in Table 5.

Table 5 ISM plan.

Action	***Target date***
Review and revise risk assessment and mitigating security controls.	Performed annually
Review and revise existing policies and procedures	Performed annually
Develop new policies and procedures	As required
Propose closer coordination procedures of the federated security teams	By end of 2019
Deploy the agreed coordination processes of the federated security teams	By end of 2020
Definition and evaluation of rapid response mechanisms for security incidents	During PY2

4.7 Incident and Service Request Management, Problem Management

The current helpdesk system (the ticketing system xGUS) used as the base for the ISRM and PM procedures needs to be integrated with the different infrastructures taking into account their own level of integration within EOSC e-infrastructure. This is the main point to be defined during the next months of the project. The first step on this integration phase is the integration of EGI and EUDAT ticketing systems in the xGUS, to be able to use the EOSC-hub helpdesk system as the main contact point for their users.

Table 6 ISRM/PM plan

Action	***Target date***
Definition of the scope	Nov 2018
Definition and deployment of the tools required for the processes ISRM and PM (ticketing system)	Nov 2018
Finalisation of the procedures	Jan 2019
Definition of the requirements and how to implement the Known Error Database, if possible within the xGUS ticketing system	Feb 2019
Define how to integrate the Incidents service request management and the problem management procedures with the different providers with different levels of integration.	March 2019

4.8 Configuration Management

The scope of the configuration management process has already been defined together with the identification of the Configuration Management Database (CMDB). The EOSC-hub CMDB is a distributed DB composed by the GOCDB and DPMT, provided jointly by EGI and EUDAT. This means that procedures for the Configuration Management should come from either GOCDB or DPMT. Software versions are automatically checked and centrally provided by the service version monitoring software SVMON.

Based on the CONFM scope, the CI types and attributes needed to run the EOSC services were defined together with a proposal for a new topology. An evaluation of both GOCDB and DPMT to implement the new CMDB topology was done resulting in the creation of a configuration management plan including the supporting technology / tools.

Table 7 CONFM plan

Action	***Target date***
DB is in place together with procedures; scope of CONF is clearly stated	Nov 2018
Definition of the CI types and attributes needed to run the EOSC service were defined	Nov 2018
Creation of configuration management plan	Dec 2018
First prototype (without functionality)	March 2019
Fully working prototype	Second semester of 2019[29]

4.9 Change Management

An initial setup of the CHM process has been defined, which will be tested and improved in an increasingly operational environment throughout the next months. This might lead to an extension of the various procedures, as well as the setup of policies in more detail. Examples can include the decision how to treat already approved standard changes of Federation Members, or how to define the best way of communication and to improve the interaction with other EOSC-hub processes.

Table 8 CHM plan

Action	***Target date***
Finalization of procedures and policies	Oct 2018
JIRA is set up and CAB working	Nov 2018
Check, refinement and improvement of existing procedures and set up	March 2019

4.10 Release and Deployment Management (RDM)

The RDM release policy is already defined together with the criteria for identifying different types of releases, such as major releases, minor releases or emergency releases. Since the RDM operates in conjunction with the CHM the RDM status was implementing in the JIRA CHM workflow allowing a better integration of both process.

[29] Currently services under the scope of the CHM are integrated in the current CMDB configuration composed by GOCDB and DPMT.

In the following table there is a list of actions that we plan to complete in the coming months in order to fully implement the process:

Table 9 RDM plan

Action	***Target date***
Policy for RDM is defined and procedures are in place	Nov 2018
JIRA is set up	Nov 2018
Full implementation of the releases and deployment plan	Dec 2018

5 Conclusion

The aim of this deliverable is to present a roadmap of the operational infrastructure within EOSC-hub. Specifically, the document provides an overview of the initial state of operations within the participating key e-Infrastructures at the beginning of the project that have been selected as the basis of the EOSC operation framework, the work done up to the writing of this deliverable, and finally the plans until the end of the project, as they are currently defined.

Furthermore, this document presents the on-going operations coordination work covering harmonization activities and plans for service delivery within the project, in addition to the IT Service Management processes that are being developed. Although the immediate scope of both of these components is the EOSC-hub project, an underlying theme for this work is to provide best practices and guidelines that are suitable and fit-for-purpose for the future EOSC as a long-term sustainable solution for all stakeholders.

Appendix I. Service Maturity (TRL7, 8 and 9)

The following guide includes proposed characteristics to help assessing the TRL level of a service. These definitions are results of the EOSC-hub RoP TF but still need to be discussed and agreed with eInfraCentral.

TRL 7

EC definition: "System prototype demonstration in operational environment"

- Service has passed through development and is an advanced stage of pre-production: the software is stable, reliable and has been deployed in an operational environment
- Functionality as required by the target user is documented, understood, validated with target sample users and accepted by them. Internal documentation exists regarding preliminary validation tests.
- An assessment has been made of the required load of the system once the transition into production is complete and a plan has been made to service this load. This assessment has been documented.
- An SLA is optional.

TRL 8

EC description: "System complete and qualified"

- There are users who are making real use of the service and rely on it for their work.
- Service documentation for end-users exists and is made available.
- An acceptable use policy/terms of use/SLA is in place
- Evidence that the service is being delivered in a way consistent with user expectations
- Provision is made for user support, with response to incident and problem management

TRL 9

EC description: "Actual system proven in operational environment"

- All requirements of TRL 8 are met.
- Customer feedback is gathered and documented. The service has been in a production state and relied upon by users for at least 1 year and evidence is provided to show this.
- There are quantitative outputs as a direct result of the service usage.