D4.1
Operational requirements for the services in the catalogue

Lead Partner:	EGI Foundation
Version:	1.7
Status:	FINAL
Dissemination Level:	PUBLIC
Document Link:	https://documents.egi.eu/document/3342

Deliverable Abstract
This document summarizes the common requirements and recommendations that will be applied to the services in the European Open Science Cloud EOSC-hub catalogue to be considered production, be exposed to the users, and to be integrated with the EOSC-hub operations infrastructure.

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

COPYRIGHT NOTICE

This work by Parties of the EOSC-hub Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EOSC-hub project is co-funded by the European Union Horizon 2020 programme under grant number 777536.

DELIVERY SLIP

	Name	***Partner/Activity***	***Date***
From:	Matthew Viljoen	EGI Foundation	20 Jul 2018
Moderated by:	Malgorzata Krakowian	EGI Foundation	
Reviewed by	Malgorzata Krakowian Daniele Spiga Carl-Fredrik Enell	EGI Foundation INFN EISCAT	
Approved by:	AMB		31 Jul 2018

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author***
v.1.0	13 Jun 2018	Version for review	Matthew Viljoen (EGI Foundation)
v.1.1	28 Jun 2018	Incorporation of feedback from reviewers	Matthew Viljoen (EGI Foundation)
v1.3	4 Jul 2018	Incorporation of further feedback and improvements	Matthew Viljoen (EGI Foundation)
v1.5	6 Jul 2018	Added Customer Relationship Management process	Matthew Viljoen (EGI Foundation)
v1.7	20 Jul 2018	Introduced concept of High, Middle and Low Level integration for the external catalogue	Matthew Viljoen (EGI Foundation)

TERMINOLOGY

Terminology in this document follows that which is defined in the FitSM-0 standard [1], which includes full definitions. A glossary including terminology for the EOSC-hub project is also available for reference [12].

Contents

Executive summary

This document outlines the operational requirements and recommendations for services wishing to join the European Open Science Cloud (EOSC-hub) Service Catalogue. It is intended primarily for Service Providers, both existing and potential future providers, wishing to participate in the European Open Science Cloud (EOSC). Service Providers may be internal to the EOSC-hub project (run by participating e-Infrastructures, partners or Thematic Services) or completely external to EOSC-hub but wanting to benefit from the single portal to services offered by the EOSC-hub project. It should be noted that the operational requirements are only one aspect of the more general Rules of Participation.

This document defines three different operational levels of integration with the Hub:

- High: the service is operated according to the EOSC-hub SMS. The service provider actively participates to the Hub Operations Coordination.
- Medium: aimed at services run with a more mature Service Management Framework
- Low: aimed at services run with a less mature Service Management Framework

For each level of integration, a set of operation requirements have been defined.

Furthermore, EOSC-hub services have been classified in two main classes, access enabling services, needed to operate the EOSC-hub itself, and researches enabling services, user facing services offered to users and research communities by means of the EOSC-hub Marketplace. The researchers enabling services can be further split in Common services, which can be re-used by other services (e.g. EGI Cloud Compute or EUDAT B2SAFE), and other researchers enabling services (e.g. a scientific application offered by a Research Infrastructure). For each of the identified service classes a minimum level to be compliant to have been identified. This can be translated on a set of operational requirements according to the level definition:

- **Access enabling services:** must satisfy the requirements of the level of integration *High*.
- **External catalogue, researchers enabling services:**
    - **Common services:** must satisfy the requirements of the level of integration *Medium*.
    - **Other research enabling services:** must satisfy the requirements of the level of integration *Low*.

Finally, it should be noted that this document started being written at a relatively early stage of development of the EOSC-hub project, at a time when many of the service management process details were still being defined and at early stages of their implementation. As such, the requirements and recommendations outlined in this document should not be regarded as final and are subject to change over the course of the project as work evolves.

1. Introduction

This document outlines the operational requirements and recommendations for services intending to join the EOSC-hub Service Catalogue. It is intended primarily for Service Providers, both existing and potential future providers wishing to participate in the European Open Science Cloud.

This work has been carried out as part of the Rules of Participation task force within the EOSC-hub project, which aims to define the conditions for service providers to offer services through the EOSC-hub. The work is primarily focused on the Operations Coordination and Federated Service Management activities in WP4. Federated Service Management within EOSC-hub is based on FitSM [1], a lightweight open family of standards which is itself based on ITIL [2].

Although the title of this deliverable implies a single service catalogue, at an early stage of the EOSC-hub project it was decided that there should be *two* service catalogues, the external and internal service catalogues, containing the production services from the external and internal service portfolios respectively:

- The *external service portfolio* which contains the services (researches enabling services) that are offered to users and research communities by means of the EOSC-hub Marketplace [13], an entry point to the EOSC-hub where users can browse and order services.
- The *internal service portfolio* is the set of access enabling services needed to operate the EOSC-hub itself. As such, these services may not be 'ordered' by users.

This document defines three different operational levels of integration with the Hub:

- High: the service is operated according to the EOSC-hub SMS. The service provider actively participates to the Hub Operations Coordination.
- Medium: aimed at services run with a more mature Service Management Framework
- Low: aimed at services run with a less mature Service Management Framework

Although each service provider is free to choose the level of integration it prefers, clearly, there are different minimal operational requirements for services depending on the type of service and whether it is destined for the external or internal service catalogue. Furthermore, services that can be used as building blocks for many researches enabling services (e.g. services from e-infrastructure like EGI Cloud Compute, EUDAT B2SAFE, etc.) need to have a tighter integration with the Hub, we call them *common services*.

According to this, we defined the following minimum requirements for service classes:

- **Internal catalogue, access enabling services** necessary for the operation of the EOSC-hub: these services must satisfy the requirements of the level of integration *High*.
- **External catalogue, researchers enabling services:**
    - **Common services:** these services must satisfy the requirements of the level of integration *Medium*. These services must be operated with a mature Service Management Framework. **Other research enabling services:** these services must satisfy the requirements of the level of integration *Low*. These services can be operated with a less mature Service Management Framework

This deliverable will aim at clarifying the operational requirements for the different classes of services within the two service catalogues, in the hope that it will be useful for current and prospective providers of services to join EOSC-hub.

The process of providing operational requirements to the project while setting up new services is also currently being defined. However, it is likely that this will take place in the form of a ticket to the EOSC-hub helpdesk or EOSC-hub JIRA instance, which will facilitate the tracking and communication required in adding new services to the Service Catalogue. If appropriate, this process may then be streamlined as much as possible to facilitate joining the catalogue from the point of view of new service providers and of staff working within the project.

Finally, it should be noted that this document started being written at a relatively early stage of development of the EOSC-hub project, at a time when many of the service management process details were still being defined and at early stages of their implementation. As such, the requirements and recommendations outlined in this document should not be regarded as final and are subject to change over the course of the project as work evolves. However, to maximize the usefulness of the information, the authors have attempted to focus on concrete minimal requirements that are unlikely to change to any large extent. As the project develops, the operational requirements, recommendations and procedures for entry into the Service Catalogue will be fully documented on the project website [4] which will remain the definitive and updated source of information.

This document outlines requirements and to reduce uncertainty uses standard key words as described in RFC2119 [5]. The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

2. Service Categories

This section maps the different EOSC-hub classes of services to three operation levels of integration. The outcome of this mapping will determine the minimal operational requirements of the service.

Details about the operational requirements for a service to be compliant with the levels of integration *High*, *Medium* and *Low* are provided respectively in section 4, section 5 and section **Error! Reference source not found.**.

2.1 Internal Catalogue – Access enabling services

Access enabling services are services necessary for the operation of the EOSC-hub and require the highest level of service integration and demand the highest operational requirements by EOSC-hub (level of integration *High*). These services are delivered by the project using the Service Management System (SMS) developed as part of the project, and include services like for example the Marketplace, the EOSC-hub Helpdesk and Authentication and Authorization Infrastructure (AAI) services

2.2 External Catalogue – Researches enabling services

2.2.1 Common services

The common services can be used as building blocks for many researches enabling services and can interoperate with other EOCS-hub services (e.g. to implement a given workflow). Examples of services which fall into this category are B2SAFE by EUDAT, online storage at EGI and the PaaS Orchestrator, developed by INDIGO DataCloud and run by an EGI partner. Other services in this category are listed as part of the existing EOSC-hub Service Catalogue [15].

Common services in the External Catalogue require a level of integration *Medium*. Indeed, they must satisfy a lower level of integration than the Access Enabling Services in the Internal Catalogue but still require the services to be delivered as part of a mature SMS meeting the requirements of FitSM [1]. This SMS will be run by the organization delivering the service, using their own operational processes and procedures. Such services will need to meet a number of operational requirements in order to enter the Service Catalogue.

2.2.2 Others Researches enabling services

The final category includes other Researches Enabling services in the External Catalogue that are mainly offering features for the end users. Usually, there are no other services in the catalogue that depend from these services. For this class of services, the minimal requirement is joining the level of integration *Low*.

Such services may wish to benefit from the single access hub and the supporting services provided by the EOSC-hub project for the benefit of their users. In joining the EOSC-hub, services in this category may be discovered along with other services in a consistent fashion through the

Marketplace, and users may be offered other benefits such as the EOSC-hub helpdesk, a standard access workflow and other user support mechanisms. The entry bar for external services to join the Marketplace is the easiest to achieve of all levels of service integration. While there are some concrete operational requirements, in many cases only recommendations exist driven from best practice deriving from Service Management standard practice.

Examples of such services may be domain-specific services or other services run by an SME or not-for-profit organization that may be of interest to others. Any services may be considered: from generic data to computing services to bespoke services such as offering virtual research environments. EOSC-hub offers the possibility of greater visibility of such services within the EOSC-hub Marketplace.

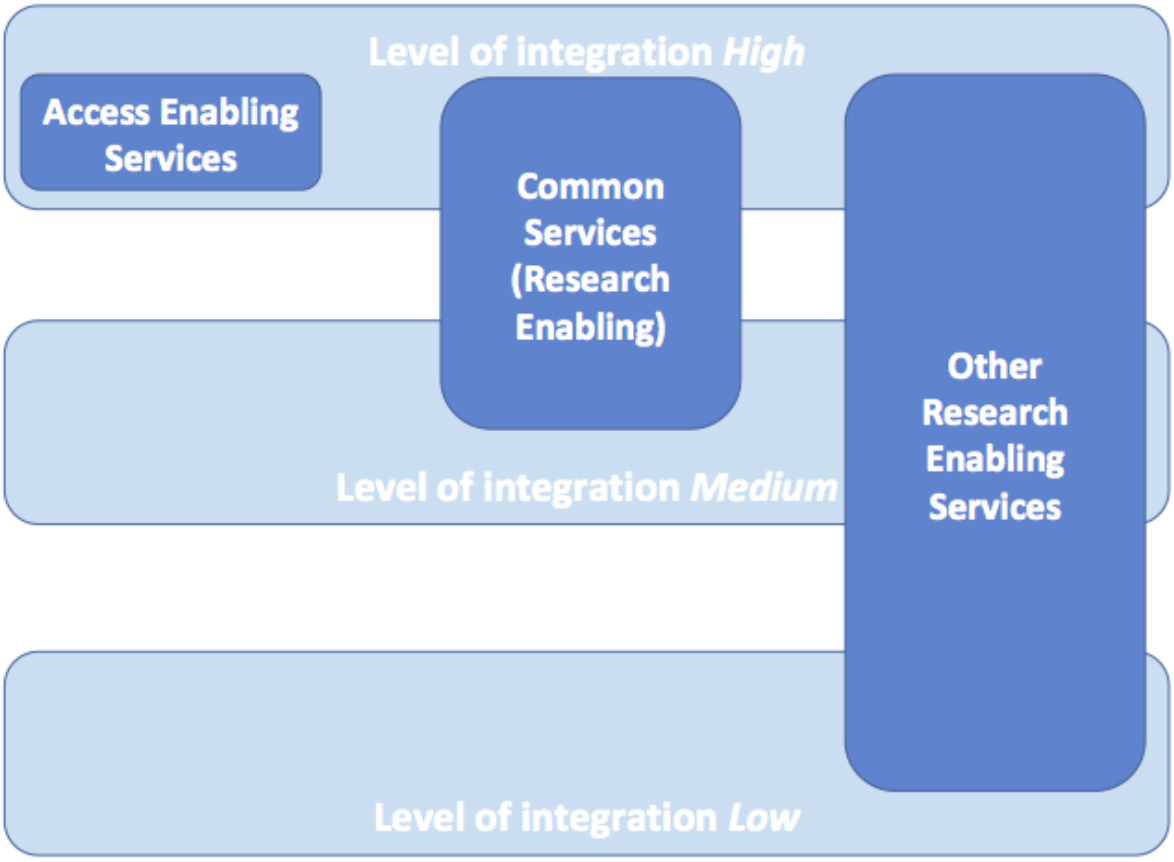

Figure 1. Possible operational levels of integration according to the classes of services.

3. Service Management System Processes

In this section we will be introducing the concept of Operational Coordination within the EOSC-hub project in addition to the main processes of IT Service Management in turn, before we examine the requirements for each of the service categories in turn.

The processes are based on FitSM [1], a free standard family for lightweight IT Service Management. It is also the standard which service management in EOSC-hub is based on.

For convenience, the FitSM process requirements have been added to the sub-sections introducing the different processes, although please note that the alignment of requirements with FitSM depends on the level of integration of the services with the EOSC-hub project – these are explored in more depth in the following chapters.

3.1 Operations Coordination

Depending on their level of integration of services into EOSC-hub, the delivery of services is coordinated by the project. For each of the three operational levels of integration defined, next sections outline the requirements of such coordination of operations activities at different levels of integration. Please note that there are multiple aspects of operations coordination which draw from the procedures defined in the separate Service Management System processes. Some examples of these are:

- Agreement of Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) and the monitoring and enforcing of target levels of service as a result of such agreements
- Management and scheduling of changes to services
- Availability and capacity considerations
- User support and problem management
- Management of security incidents
- Definition of operational procedures with roles and responsibilities

In the cases of services in the external catalogue, it will be seen that there are operations requirements for the different processes but no explicit requirements for operations coordination, apart from signing up to the Operations Coordination mailing list run by the project [16] – further details of how operations activities are coordinated is delegated to the service provider. This of course does not imply that operations coordination is not a critical part of proper service delivery – it just means that there are no explicit requirements.

3.2 Service Portfolio Management

FITSM REQUIREMENTS
• PR1.1 A service portfolio shall be maintained. All services shall be specified as part of the service portfolio. • PR1.2 Design and transition of new or changed services shall be planned. • PR1.3 Plans for the design and transition of new or changed services shall consider timescales, responsibilities, new or changed technology, communication and service

acceptance criteria. • PR1.4 The organisational structure supporting the delivery of services shall be identified, including a potential federation structure as well as contact points for all parties involved. • PR2.1 A service catalogue shall be maintained.

The goal of the Service Portfolio Management (SPM) process is to manage the service portfolio of the EOSC-hub in order to ensure that all services are specified, major changes are reviewed and approved according to the most suitable decision-making process and criteria, and that the related service catalogues are derived and aligned.

All services will be described in the service portfolio following an agreed template that is currently being defined (https://wiki.eosc-hub.eu/display/EOSC/Service+Portfolio+Entry+Template). There will be also the definition of a service lifecycle and, for each of the agreed maturity phases, there will be a check-list defined that needs to be verified in order to approve a service in the related phase (see https://wiki.eosc-hub.eu/display/EOSC/Service+Phases).

The initial version of SPM proposes to scope two different service portfolios that will be managed under different governance structures:

- EOSC-hub service portfolio: composed of the researches enabling/customer-facing services that are offered by the EOSC-hub
    - The evolution of this portfolio is regulated by the EOSC-hub Rules of participations that are being defined by a dedicated EOSC-hub Task Force also taken into account input from other initiatives (e.g. HLEG EOSC, EOSC-pilot, OpenAIRE, RDA, and eInfraCentral projects). The procedure SPM1 [9] ensures that all requests for major changes to the service portfolio are validated and that all the necessary actions are taken to ensure a proper propagation of the changes within the EOSC-hub. The information to submit a major change to the service portfolio will be requested via a dedicated service change request form.
    - EOSC-hub internal service portfolio: composed of the Access Enabling Services needed to operate the EOSC-hub. The evolution of this portfolio is closely controlled by the EOSC-hub governance. The procedure SPM2 [10] ensures that major changes with risk to have a major financial consequence for the EOSC-hub initiative need the EOSC-hub Project Management Board approval. Service providers need to comply with a set of policies for the internal services that needs to be defined. The information to submit a major change to the service portfolio will be requested via a dedicated form called a Service Design and Transition Package (SDTP).

This process will also be responsible for Service Catalogue although this activity is part of Service Level Management process in FitSM standard. This change has been introduced due to definition of Work packages in EOSC-hub project.

3.3 Service Level Management

FITSM REQUIREMENTS
• PR2.2 For all services delivered to customers, SLAs shall be in place. • PR2.3 SLAs shall be reviewed at planned intervals.

- PR2.4 Service performance shall be evaluated against service targets defined in SLAs.
- PR2.5 For supporting services or service components provided by federation members or groups belonging to the same organisation as the service provider or external suppliers, OLAs and UAs shall be agreed.
- PR2.6 OLAs and Uas shall be reviewed at planned intervals.
- PR2.7 Performance of service components shall be evaluated against operational targets defined in OLAs and Uas.

Service Level Management (SLM) is the framework whereby services are defined and service levels are agreed in the form of Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) are established.

In the context of EOSC-hub, the service catalogue is managed by the SPM process in WP2 together with the service portfolio. This process will focus on establishing SLAs (with customers), OLAs (with providers within EOSC-hub project) and Uas (with providers that are not part of EOSC-hub project). Based on the experience of EGI and EUDAT, it was decided that SLAs will be established on a per-customer basis since, in the majority of the cases, the customer will request a number of services with a customized set up. In special cases, a corporate SLA could be also defined (e.g. for services that do not customisations). The coordination of delivery of those sets of services will be executed in collaboration with the CRM process.

Service Reporting Management (SRM)
FITSM REQUIREMENTS
• PR3.1 Service reports shall be specified and agreed with their recipients. • PR3.2 The specification of each service report shall include its identity, purpose, audience, frequency, content, format and method of delivery. • PR3.3 Service reports shall be produced. Service reporting shall include performance against agreed targets, information about significant events and detected nonconformities.

In addition, this process will be responsible for activities defined by FitSM as part of Service Reporting Management. Service reports are planned for all SLAs agreed via EOSC-hub marketplace.

3.4 Customer Relationship Management

FITSM REQUIREMENTS
• PR7.1 Service customers shall be identified. • PR7.2 For each customer, there shall be a designated contact responsible for managing the customer relationship and customer satisfaction. • PR7.3 Communication mechanisms with customers shall be established.

- PR7.4 Service reviews with the customers shall be conducted at planned intervals.
- PR7.5 Service complaints from customers shall be managed.
- PR7.6 Customer satisfaction shall be managed.

Customer relationship management process will be run and coordinated centrally. It will be responsible for maintaining good relationship with customers who ordered services via EOSC-hub marketplace as well as for order management.

All service providers are expected to work closely and support the process to fulfil process requirements.

3.5 Supplier Relationship Management

FITSM REQUIREMENTS
• PR8.1 Suppliers shall be identified. • PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with the supplier. • PR8.3 Communication mechanisms with suppliers shall be established. • PR8.4 Supplier performance shall be monitored.

In the case of EOSC-hub service delivery, within Supplier Relationship Management (SUPPM), a 'supplier' refers to either the service provider of the service, or the provider of the software or supporting component needed by the service provider to provide the service to their customer or users. From the point of view of the EOSC-hub project, suppliers refer to the service providers, whereas from the point of view of the service providers themselves, suppliers refer to the providers of the software or supporting component. SUPPM ensures that an optimal relationship is maintained between the project and the service providers, and between the service providers and the providers of software and supporting components.

3.6 Configuration Management

FITSM REQUIREMENTS
• PR11.1 Configuration item (CI) types and relationship types shall be defined. • PR11.2 The level of detail of configuration information recorded shall be sufficient to support effective control over Cis. • PR11.3 Each CI and its relationships with other Cis shall be recorded in a configuration management database (CMDB). • PR11.4 Cis shall be controlled and changes to Cis tracked in the CMDB. • PR11.5 The information stored in the CMDB shall be verified at planned intervals. • PR11.6 Before a new release into a live environment, a configuration baseline of the affected Cis shall be taken.

The goal of Configuration Management (CONFM) is to provide and maintain a logical model of all configuration items and their relationships and dependencies. Each service should be defined by one or more sets of items (variables) together with the relationship between them.

3.7 Change Management

FITSM REQUIREMENTS
• PR12.1 All changes shall be registered and classified in a consistent manner. • PR12.2 All changes shall be assessed and approved in a consistent manner. • PR12.3 All changes shall be subject to a post implementation review and closed in a consistent manner. • PR12.4 There shall be a definition of emergency changes and a consistent approach to managing them. • PR12.5 In making decisions on the acceptance of requests for change, the benefits, risks, potential impact to services and customers and technical feasibility shall be taken into consideration. • PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes, and proposed deployment dates, which shall be communicated to interested parties. • PR12.7 For changes of high impact or high risk, the steps required to reverse an unsuccessful change or remedy any negative effects shall be planned and tested.

The purpose of Change Management (CHM) is to ensure that changes to configuration items are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services. According to FitSM, all changes should be planned, classified and deployed following a procedure. In addition, the deployment should follow a pre-defined schedule.

3.8 Release and Deployment Management

FITSM REQUIREMENTS
• PR13.1 A release policy shall be defined. • PR13.2 The deployment of new or changed services and service components to the live environment shall be planned with all relevant parties including affected customers. • PR13.3 Releases shall be built and tested prior to being deployed. • PR13.4 Acceptance criteria for each release shall be agreed with the customers and any other relevant parties. Before deployment the release shall be verified against the agreed acceptance criteria and approved. • PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers. • PR13.6 Releases shall be evaluated for success or failure.

Release and Deployment Management (RDM) ensures that releases are controlled and deployed in a consistent manner. This is done by ensuring a systematic approach to defining a release as a collection of one or more Configuration Items (Cis) that are adequately tested before being deployed to the live production environment.

3.9 Service Availability and Continuity Management

FITSM REQUIREMENTS
• PR4.1 Service availability and continuity requirements shall be identified taking into consideration SLAs. • PR4.2 Service availability and continuity plans shall be created and maintained. • PR4.3 Service availability and continuity planning shall consider measures to reduce the probability and impact of identified availability and continuity risks. • PR4.4 Availability of services and service components shall be monitored.

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 covers the availability and the reliability of a service and its components, which is done by monitoring in order to promptly intervene when an incident occurs. Performance reports are produced periodically to provide analysis of problems that have happened and to help to propose plans and solutions for improving the availability of services.

At the same time this process covers regular risk assessment and management exercises to reduce risks to services to agreed acceptable levels and to plan and prepare for their recovery.

The result of these activities is the creation of a Service Availability and Continuity Plan 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. The plan should also comprise an availability and continuity test to verify the robustness of the adopted measures and of the service recovery procedures.

3.10 Capacity Management

FITSM REQUIREMENTS
• PR5.1 Service capacity and performance requirements shall be identified taking into consideration SLAs. • PR5.2 Capacity plans shall be created and maintained. • PR5.3 Capacity planning shall consider human, technical and financial resources. • PR5.4 Performance of services and service components shall be monitored based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.

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

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

The plan clearly specifies any assumptions made as well as any recommendations quantified in terms of resources required, cost, benefits, impact, etc.

3.11 Information Security Management

FITSM REQUIREMENTS
• PR6.1 Information security policies shall be defined. • PR6.2 Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks. • PR6.3 Information security policies and controls shall be reviewed at planned intervals. • PR6.4 Information security events and incidents shall be given an appropriate priority and managed accordingly. • PR6.5 Access control, including provisioning of access rights, for information-processing systems and services shall be carried out in a consistent manner.

Information Security Management (ISM) develops and implements the policies and procedures required to ensure consistent and coordinated security operations across the services provided in the catalogue. All this is aimed at managing security risks, protecting the assets of EOSC-hub and contributing to the maintenance of the confidentiality, integrity and availability of Services and Data.

3.12 Incident and Service Request Management

FITSM REQUIREMENTS
• PR9.1 All incidents and service requests shall be registered, classified and prioritized in a consistent manner. • PR9.2 Prioritization of incidents and service requests shall take into account service targets from SLAs. • PR9.3 Escalation of incidents and service requests shall be carried out in a consistent

manner.

- PR9.4 Closure of incidents and service requests shall be carried out in a consistent manner.
- PR9.5 Personnel involved in the incident and service request management process shall have access to relevant information including known errors, workarounds, configuration and release information.
- PR9.6 Users shall be kept informed of the progress of incidents and service requests they have reported.
- PR9.7 There shall be a definition of major incidents and a consistent approach to managing them.

Incident and Service Request Management (ISRM) develops and implements the policies and procedures required to react to operational incidents across the services provided in the catalogue. The main objective is to restore the agreed service operation within the agreed time after the occurrence of an incident, and to respond to user service requests within the EOSC-hub infrastructure.

3.13 Problem Management

FITSM REQUIREMENTS
• PR10.1 Problems shall be identified and registered based on analysing trends on incidents. • PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on the services. • PR10.3 If a problem is not permanently resolved, a known error shall be registered together with actions such as effective workarounds and temporary fixes. • PR10.4 Up-to-date information on known errors and effective workarounds shall be maintained.

Problem Management (PM) develops and implements the policies and procedures required to track and minimize the occurrence of incidents. The main objective is to investigate the root causes of incidents in order to avoid future recurrence of incidents by resolving the underlying causes, or to ensure that workarounds or fixes are available within the services provided by the EOSC-hub.

4. Level of integration *High*

This section examines the requirements for EOSC-hub services belonging to the level of integration *High*.

Requirements described in this section are the minimal requirements that must be satisfied by the Access Enabling Services part of the EOSC-hub internal service catalogue.

4.1 Operations Coordination

Each service belonging to the level of integration *High* SHALL meet the following criteria:

- A person is nominated with overall responsibility of the service who should sign up to the Operations Coordination mailing list run by the project [16]. In the case of separate instances of the same service running in the e-Infrastructure, an additional person is nominated with responsibility for each instance (or instances) of the service.
- Service providers representative participate in the activities of the Operations Management Board to be aware of news regarding the operational status of services in the EOSC-hub and to disseminate operational information relevant to others in EOSC-hub.
- Ensure that operations is overseen by EOSC-hub governance
- Be fully compliant with policies defined in EOSC-hub Service Management System.

4.2 Service Portfolio Management

Access enabling services will be (re-)evaluated against the SPM2[10] procedure. All future major changes will also be evaluated and approved following this procedure.

Researches enabling services will be (re-)evaluated against the SPM1[10] procedure. All future major changes will also be evaluated and approved following this procedure.

4.3 Service Level Management

Services shall agree on Operation Level Agreement (OLA) with EOSC-hub to ensure delivery of those services. Services from external catalogue shall also agree on Operation level agreements supporting Service Level agreements with customers. .
To set up OLAs, a number of information shall be provided in addition to information gathered in Service portfolio.
Template for OLA and SLA agreements will be defined based on FitSM standard and experience of the project participants.

4.4 Customer Relationship Management

Each provider SHALL:

- Follow and support the EOSC-hub Customer Relationship Management process.

4.5 Supplier Relationship Management

Services providers SHALL:

- Identify all suppliers and maintain a list of service provider contact details. Each service provider SHALL have a contact at the participating e-Infrastructure.
- Monitor Service Provider performance, e.g. responsiveness to problems raised against their service, readiness to apply patches for security problems etc.
- Identify a security contact for each Service Provider who can be contacted in case of a security problem with their service.

4.6 Configuration Management

Services providers SHALL:

- Undergo the Configuration Management process carried on by the EOSC-hub, which will maintain a CMDB for storing the information of all the configuration items (CI) related to the services.
- Provide the necessary information for the definition of the Cis corresponding to the services and their relationship, as requested by the EOSC-hub, with a sufficient level of detail to allow an effective control over all the Cis.
- Verify periodically or upon request by the EOSC-hub the information stored in the CMDB.

4.7 Change Management

Services providers SHALL:

- Follow the EOSC-hub change management process.
- Classify the changes according to the EOSC-hub policies.
- Require plans to document and evaluate high impact changes. The evaluation should take into account the following items:
    - Benefits
    - Risk Assessment
    - Potential impact across infrastructure
    - Technical feasibility
    - Effort / cost
- Require that high impact changes are evaluated by the Service Owner and communicated to the EOSC-hub Change Advisory Board (CAB).
- Define emergency release procedures.

4.8 Release and Deployment Management

Services providers SHALL:

- Follow the release and deployment procedure in practice for EOSC-hub. Details of the procedure may change later but will consist of the following steps:
    - Deployment of new or changed services and service components to the live environment SHALL be planned with all relevant parties including affected customers.
    - Releases SHALL be built and tested prior to being deployed.
    - Agree acceptance criteria for each release with the customers and any other relevant parties. Before deployment the release SHALL be verified against the agreed acceptance criteria and approved.

- Consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers during deployment preparation. A contingency plan SHALL be considered for major updates.
- Evaluate releases against success or failure criteria with the information reported to the CHM process.

4.9 Service Availability and Continuity Management

EOSC-hub will create and maintain Service Availability and Continuity Plans for every service in the catalogue with level of integration *High*. In order to allow this, services providers SHALL:

- Allow the EOSC-hub monitoring framework to monitor the status of the service through the execution of service specific tests in order to detect any failure and to produce Availability and Reliability reports.
- Periodically perform risk assessment and management exercises to identify risks to the availability and continuity of the service, planning adequate measures to reduce their impact and probability.

4.10 Capacity Management

EOSC-hub will create and maintain Service Capacity Plans for every service in the catalogue with level of integration *High*. In order to allow this, services provider SHALL:

- Allow EOSC-hub to monitor the performances of services and services components based on the capacity utilization, identifying operational warnings and exceptions.

4.11 Information Security Management

Services provider SHALL:

- Abide by the requirements of all approved and adopted EOSC-hub Security Policies and Procedures [11].

4.12 Incident and Service Request Management

Services provider SHALL:

- Integrate the service helpdesk into the EOSC-hub helpdesk system.
- Keep track of the incidents received and the contact with the users (ticketing system).
- Fulfil any OLA related with the EOSC-hub support service.
- 2nd level support for the service needs to be provided.
- Follow the guidelines created for the EOSC-hub support. These guidelines are currently being prepared and will be available from the project wiki [4].

4.13 Problem Management

Services provider SHALL:

- Contribute to identification of problems and evaluation of identified problems in order to define workarounds and solutions.

5. Level of integration *Medium*

This section examines the requirements for EOSC-hub services belonging to the level of integration *Medium*.

Requirements described in this section are the minimal requirements that must be satisfied by the Common Services part of the EOSC-hub external service catalogue (Researches Enabling Services).

5.1 Operations Coordination

Organizations delivering services in the External Catalogue are expected to run all operational coordination activities related to delivering their services. However, each service of the EOSC-hub catalogue belonging to the level of integration *Medium* SHALL meet the following criteria:

- A person is nominated with overall responsibility of the service, who should sign up to the Operations Coordination mailing list run by the project [16]. In the case of separate instances of the same service running in the e-Infrastructure, an additional person is nominated with responsibility for each instance (or instances) of the service
- Service providers representative participate in the activities of the Operations Management Board to be aware of news regarding the operational status of services in the EOSC-hub and to disseminate operational information relevant to others in EOSC-hub.

5.2 Service Portfolio Management

Providers who are partners of the EOSC-hub have been pre-selected during the preparation phase via an open call mechanism. They are currently providing services that are part of either the EOSC-hub service portfolio or the EOSC-hub internal service portfolio. Once the procedures SPM1 [9] and SPM2[10] are completed with the rules of participations and other important aspects, they will be re-evaluated and aligned to make sure they comply with them.

5.3 Service Level Management

Each e-service provider SHALL:

- Establish internally operation level agreements, where needed, to support delivery of the services
- Provide necessary information needed to set up service level agreements (SLA) for orders registered in EOSC-hub Marketplace and fulfil those orders.
- Agree on operation level agreement with EOSC-hub to ensure delivery of those services.

5.4 Customer Relationship Management

Each service provider SHALL:

- Implement and follow a Customer Relationship Management process.
- Support the EOSC-hub Customer Relationship Management process.

5.5 Supplier Relationship Management

Each service provider SHALL:

- Identify all suppliers and maintain a list of service provider contact details. Each service provider SHALL have a contact person.
- Monitor Service Provider performance, e.g. responsiveness to problems raised against their service, readiness to apply patches for security problems etc.
- Identify a security contact for each Service Provider who can be contacted in case of a security problem with their service.

5.6 Configuration Management

Each service provider SHALL:

- Maintain a CMDB for storing the information of all the configuration items related to the services offered through the EOSC-hub service catalogue, as well as the relationship between them.
- Define Cis types corresponding to the services and relationship types between them, with a sufficient level of detail to allow an effective control over all the Cis.
- Track in the CMDB changes to the Cis.
- Implement procedures to check periodically the validity of the information stored in the CMDB.
- Take a snapshot of the configuration baseline of the affected Cis before a new release.

5.7 Change Management

Each service provider SHALL:

- Ensure that changes to configuration items are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services.
- All changes SHALL be planned, classified and deployed according to a procedure

5.8 Release and Deployment Management

Each service provider SHALL:

- Implement an internal release and deployment management process containing the following steps:
    - Plan all releases in advance and in case of major changes inform EOSC-hub responsible group.

    - Software releases SHOULD be built using an internal / external repository based on a distributed version control system.
    - Validate the release prior to announcement.
    - Create and maintain adequate documentation.
    - Deploy and review release and in case of unsuccessful changes be ready to apply remedy or revert changes.
- Announce planned maintenance windows or interruptions at least 24h in advance to all users (and if applicable, to other service providers) following procedures that will be defined by the project [4].

Notify users (and if applicable to other service providers) of new releases following procedures defined by the project [4].

5.9 Service Availability and Continuity Management

Each service provider SHALL do the following for each service to be considered for inclusion into the EOSC-hub Service Catalogue:

- Allow the EOSC-hub monitoring framework to monitor the status of the service through the execution of service specific tests in order to detect any failure and to produce Availability and Reliability reports. In the case of services which funding is covered under Virtual Access, additional monitoring may be required to demonstrate usage of the service.

In addition to this, participating e-Infrastructures SHOULD:

- Periodically perform risk assessment and management exercises to identify risks to the availability and continuity of the service, planning adequate measures to reduce their impact and probability.
- Create and maintain Service Availability and Continuity Plans.

5.10 Capacity Management

Each service provider SHALL:

- Create and maintain Service Capacity Plans.
- Monitor the performances of services and services components based on the capacity utilization, identifying operational warnings and exceptions.

5.11 Information Security Management

Each service provider SHALL:

- Provide a contact point for communication with EOSC-hub on all matters related to ISM.
- Create and maintain a Data Privacy Policy for compliance with legal requirements related to Data Protection. A template of this will be made available for guidance [4].
- Collaborate with the EOSC-hub security teams in handling security vulnerabilities that are present in their service(s) and/or in any ongoing security incidents.

5.12 Incident and Service Request Management

Each service provider SHALL:

- Take into account the guidelines provided by the EOSC-hub helpdesk team to answer the requests of the services.
- 2nd level support for the service needs to be provided via a ticketing system to store the history of the requests and contacts between users and user support team, also the system should be able to provide the time to respond and time to resolve for each request.

5.13 Problem Management

Each service provider SHALL:

- Have a database of known errors, linked with ISRM; a ticketing system could be an option as such a tool can be used for both processes at the same time.
- Have a Problem Management procedure for the service in order to provide solutions for repetitive errors or incidents.

6. Level of integration *Low*

This section examines the requirements for EOSC-hub services belonging to the level of integration *Low*.

Requirements described in this section are the minimal requirements that must be satisfied by the other Researches Enabling Services (not Common Services) part of the EOSC-hub external service catalogue.

6.1 Operations Coordination

Organizations delivering services in the External Catalogue are expected to run all operational coordination activities related to delivering their services. However, each service of the EOSC-hub catalogue belonging to the level of integration *Medium* SHALL meet the following criteria:

- A person is nominated with overall responsibility of the service, who should sign up to the Operations Coordination mailing list run by the project [16]. In the case of separate instances of the same service running in the e-Infrastructure, an additional person is nominated with responsibility for each instance (or instances) of the service
- Service providers representative participate in the activities of the Operations Management Board to be aware of news regarding the operational status of services in the EOSC-hub and to disseminate operational information relevant to others in EOSC-hub.

6.2 Service Portfolio Management

New services or major changes to existing services in the EOSC-hub service portfolio can be proposed according to the procedure SPM1.

6.3 Service Level Management

Each provider SHOULD:

- Establish internally operation level agreements, where needed, to support delivery of the services

Each provider SHALL:

- Provide necessary information needed to set up service level agreements (SLA) for orders registered in EOSC-hub Marketplace and fulfil those orders.
- Agree on operation level agreement with EOSC-hub to ensure delivery of those services.

6.4 Customer Relationship Management

Each provider SHOULD:

- Implement and follow a Customer Relationship Management process

Each provider SHALL:

- Support the EOSC-hub Customer Relationship Management process.

6.5 Supplier Relationship Management

Service Providers SHOULD:

- Maintain a relationship with providers of software and suppliers.
- Identify all software and supporting component suppliers and maintain a list of suppliers' contact details.
- Monitoring of supplier performance, e.g. responsiveness to problems raised against the software, readiness to release patches for security problems etc.
- Identify a security contact for each supplier who can be contacted in case of a security problem with the software or supporting contact.

6.6 Configuration Management

Service Providers SHOULD implement an internal configuration management process, which should take into consideration the following:

- define a minimum set of Cis that are able to fully define a service together with the relationship between Cis in order to run the service.
- maintain a database (Configuration Management Database – CMDB) which stores all CI values and changes associated to each items. It is advisable to make a snapshot of all Cis before a new release.
- Implement internal procedures to periodically check the validity of the information stored in the CMDB.

6.7 Change Management

Service Providers SHOULD:

- Implement an internal change management process.
- Maintain a schedule of changes including dates of changes and communicate to EOSC-hub in advance of changes.

6.8 Release and Deployment Management

Service Providers SHOULD:

- Implement an internal release and deployment management process containing the following steps:
    - Plan all releases in advance and in case of major changes inform EOSC-hub responsible group.
    - Software releases SHOULD be built using an internal/external repository based on a distributed version control system.

- Validate the release prior to announcement.
- Create and maintain adequate documentation.
- Deploy and review the release and in case of unsuccessful changes be ready to apply remedy or revert changes.

In addition, external service providers SHALL notify users (and other service providers, if applicable) in advance of new releases following procedures that will be defined by the project [4].

6.9 Service Availability and Continuity Management

Service Providers SHOULD:

- Allow the EOSC-hub monitoring framework to monitor the status of the service through the execution of service specific tests in order to detect any failure and to produce Availability and Reliability reports. In the case of services whose funding is covered under Virtual Access, additional monitoring may be required to demonstrate usage of the service.
- Periodically perform risk assessment and management exercises to identify risks to the availability and continuity of the service, planning adequate measures to reduce their impact and probability.
- Create and maintain Service Availability and Continuity Plans.

6.10 Capacity Management

Service Providers SHOULD:

- Create and maintain Service Capacity Plans.
- Monitor the performances of services and services components based on the capacity utilization, identifying operational warnings and exceptions.

6.11 Information Security Management

Service Providers SHOULD:

- Provide a contact point for communication with EOSC-hub on all matters related to ISM.
- Create and maintain a Data Privacy Policy for compliance with legal requirements related to Data Protection.
- Determine and make known their willingness and ability to collaborate (or otherwise) with the EOSC-hub security teams in handling security vulnerabilities that are present in their service(s) and/or in any ongoing security incidents.

6.12 Incident and Service Request Management

Service Providers SHOULD:

- Read the guidelines for the user support provided by EOSC-hub, but they will not be mandatory for external services. These guidelines are currently being prepared and will be available from the project wiki [6].

- 2nd level support for the service needs to be provided. 2nd level support is the expert support where more in-depth help is needed to support the service. 1st level support is provided by the EOSC-hub project and aims to deal with basic problems or to re-assign problems to 2nd level support, as appropriate. Ideally this should be managed in the form of a mailing list rather than an individual person.

6.13 Problem Management

Service Providers SHOULD:

- Have a database of known errors to manage the problem management process, linked with ISRM; a ticketing system could be an option as such a tool can be used for both processes at the same time.

7. Conclusions

This document has sought to give an introduction to the operational requirements, as they are understood at this point of the project, for services wishing to join the EOSC-hub project service catalogue. It has attempted to clarify three different operational requirements of increasing levels. Service providers can choose the level of integration that best fits with their needs but a minimum level to be compliant with has been defined for the three following classes of services:

- Access enabling services: compliant with the level of integration *High*;
- Common services (a sub-set of Researches enabling services that can be re-used by other services): compliant with the level of integration *Medium*;
- Other researchers enabling services (not common services): compliant with the level of integration *Low*.

It is hoped that, although this document is unable to give definitive operational requirements, as the service management processes are still being defined, prospective service providers will be able to obtain an idea of what will be required of them to join the catalogue. The document provides links to where up to date information may be obtained as the project progresses.

Finally, it should be noted that these operational requirements will be especially useful for services wishing to benefit from the Virtual Access[14] funding mechanism whereby the service delivery needs to be provided in a consistent way across the service catalogue and the service easily discovered by users in order to show an increasing number of users over time to be eligible for the funding.

8. References

No	Description/Link
[1]	FitSM https://www.itemo.org/fitsm/
[2]	ITIL https://www.axelos.com/best-practice-solutions/itil
[3]	EOSC-pilot Deliverable D5.3 EOSC Federated Service Management Framework (under review and pending publishing at the time of writing)
[4]	EOSC-hub Service Documentation https://www.eosc-hub.eu/services/service-documentation
[5]	Key words for use in RFCs to Indicate Requirement Levels https://www.ietf.org/rfc/rfc2119.txt
[6]	EOSC-hub SMS https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+SMS
[7]	HLG-KET final report http://ec.europa.eu/DocsRoom/documents/11283/attachments/1/translations/en/renditions/native
[8]	Annex G from the WP2014-2015 program http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf
[9]	See SPM1 under https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+SMS
[10]	See SPM2 under https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+SMS
[11]	EOSC-hub Security Policies and Procedures https://www.eosc-hub.eu/services/policy-and-procedures
[12]	EOSC-hub Terminology https://confluence.egi.eu/display/EOSC/EOSC-hub+Glossary
[13]	EOSC-hub Marketplace https://marketplace.eosc-hub.eu/
[14]	Virtual Access https://wiki.egi.eu/wiki/EOSC-hub:VA-TNA_FAQ
[15]	EOSC-hub Service Catalogue https://confluence.egi.eu/display/EOSC/EOSC-hub+service+catalogue
[16]	Details of the Operational Coordination mailing list https://wiki.eosc-hub.eu/display/EOSC/T4.1+Operations+Coordination+and+Supplier+Relationship+Management

Appendix I. Overview of Operational Requirements and Recommendations

This appendix is designed to give a quick overview and comparison of the operational requirements and recommendations for the different types of services. If there are no explicit requirements for entry into the catalogue, n/a is indicated for not applicable. For more details, please refer to the main body of the text in this document corresponding to the category of interest as indicated by the section number.

Category	**Access Enabling services**	**Common services**	**Researches enabling services**
Catalogue	**Internal catalogue**	**External catalogue**	**External catalogue**
Minimal level of integration	**High**	**Middle**	**Low**
Operational Coordination (section 3.1)	SHALL: • Nominate a person running the service who is signed up to the Operations Coordination mailing list • Participate in the Operations Management Board • Ensure that operations is overseen by EOSC-hub governance • Be fully compliant with policies defined in EOSC-hub SMS (section 4.1)	SHALL: • Nominate a person running the service who is signed up to the Operations Coordination mailing list • Participate in the Operations Management Board (section 5.1)	SHALL: • Nominate a person running the service who is signed up to the Operations Coordination mailing list • Participate in the Operations Management Board (section 6.1)
Service Portfolio Management	SHALL: • Follow the EOSC-hub SLM process	SHALL: • Implement SLM process • Provide necessary	SHALL: • Provide necessary information

(section 3.2)	(section 4.2)	information (section 5.2)	(section 6.2)
Service Level Management (section 3.3)	SHALL: • Follow the EOSC-hub SLM process • Agree on an OLA with EOSC-hub (section 4.3)	SHALL • Implement SLM process • Agree on an OLA with EOSC-hub • Provide information needed to establish SLAs and commit to their fulfilment (section 5.3)	SHALL: • Agree on an OLA with EOSC-hub • Provide information needed to establish SLAs and commit to their fulfilment SHOULD • Establish internally OLAs (section 6.3)
Customer Relationship Management (section 3.4)	SHALL: • Follow and support the EOSC-hub CRM process (section 4.4)	SHALL • Implement and follow a CRM process • Support the EOSC-hub CRM process (section 5.4)	SHOULD • Implement and follow a CRM process SHALL: • Support the EOSC-hub CRM process (section 6.4)
Supplier Relationship Management (section 3.5)	SHALL: • Follow the EOSC-hub SUPPM process (section 4.5)	SHALL: • Implement and follow a SUPPM process (section 5.5)	SHOULD: • Implement and follow a SUPPM process (section 6.5)
Configuration Management	SHALL: • Follow the EOSC-hub CONFM process	SHALL: • Implement and follow a CONFM process	SHOULD: • Implement and follow a CONFM process

(section 3.6)	(section 4.6)	(section 5.6)	(section 6.6)
Change Management (section 3.7)	SHALL: • Follow the EOSC-hub CHM process (section 4.7)	SHALL: • Implement and follow a CHM process (section 5.7)	SHOULD: • Implement and follow a CHM process • Maintain a schedule of change and communicate to EOSC-hub in advance of changes (section 6.7)
Release and Deployment Management (section 3.8)	SHALL: • Follow the EOSC-hub RDM process (section 4.8)	SHALL: • Implement and follow a RDM process • Announce planned maintenance in advance • Announce new releases in advance (section 5.8)	SHALL: • Notify users before new releases SHOULD: • Plan, validate and document releases (section 6.8)
Service Availability and Continuity Management (section 3.9)	SHALL: • Follow the EOSC-hub SACM process (section 4.9)	SHALL: • Implement and follow a SACM process • Allow the monitoring of the services • Periodically perform risk assessment and management exercises (section 5.9)	SHALL: • Allow the monitoring of the services SHOULD: • Periodically perform risk assessment and management exercises (section 6.9)
Capacity Management	SHALL: • Follow the EOSC-hub CAPM process	SHALL: • Implement and follow a CAPM process • Define and	SHOULD: • Manage capacity necessary to deliver services

(section 3.10)	(section 4.10)	manage Capacity management process (section 5.10)	(section 6.10)
Information Security Management (section 3.11)	SHALL: • Follow the EOSC-hub ISM process (section 4.11)	SHALL: • Implement and follow an ISM process • Abide by EOSC-hub Security Policies and Procedures (section 5.11)	SHALL: • Abide by EOSC-hub Security Policies and Procedures (section 6.11)
Incident and Service Request Management (section 3.12)	SHALL: • Follow the EOSC-hub ISRM process (section 4.12)	SHALL: • Implement and follow an ISRM process • Be aware of guidelines for user support • Provide a support via EOSC-hub helpdesk (section 5.12)	SHOULD: • Be aware of guidelines for user support • Provide a support via EOSC-hub helpdesk (section 6.12)
Problem Management (section 3.13)	SHALL: • Follow the EOSC-hub PM process (section 4.13)	SHALL: • Implement and follow a PM process (section 5.13)	SHOULD: • Mantain a database with known errors linked to ISRM (section 6.13)

Appendix II. TRL Maturity Levels

Technology Readiness Level (TRL) is a means of systematically gauging the maturity of a technology. Originally developed for the space industry by NASA, it became later adopted by various departments of defence around the world and by others. Its use within the EU was first recommended by the High Level Group of Key Enabling Technologies (HLG-KET) final report in 2011 [7] and it was subsequently used in H2020 funding programs.

For use within the context of operational service delivery, TRL has its limitations as it is usually used to describe the maturity of underlying technologies rather than the delivery of them in the form of a service to end users. In addition to this, an end service may be the union of multiple sub-components, each based on various technologies with differing levels of maturity. Nevertheless, TRL is a widely used and easily understandable method that was included in the EOSC-hub project proposal.

The basic explanations of TRL may be seen from the definitions from the European Commission in preparation for its WP2014-2015 program [8]:

TRL 1	Basic principles observed
TRL 2	Technology concept formulated
TRL 3	Experimental proof of concept
TRL 4	Technology validated in lab
TRL 5	Technology validated in relevant environment
TRL 6	Technology demonstrated in relevant environment
TRL 7	System prototype demonstration in operational environment
TRL 8	System complete and qualified
TRL 9	Actual system proven in operational environment

During the preparation stages of the EOSC-hub project, services initially considered for inclusion in the project were built on technologies deemed to be of TRL 8 or higher and addressing interoperability needs by promoting the adoption of open standards and protocols, as confirmed within Objective 3 of the Grant Agreement (No. 777536, EOSC-hub). Services at TRL 8 are considered within EOSC-hub to be at a Production level, where it is made clear to users which functionalities are present and which are not, and users' reasonable expectations of stability are met. Such services will have passed through the previous development states of proof-of-concept, pilot and pre-production, and will have successfully proven to users that the services are mature and fit-for-purpose for their target communities.
TRL8 remains the minimal requirement to include new services in the EOSC-hub catalogue. The service assessment will include the evaluation of both operational and technical aspects. This

deliverable covered the operational requirements a service, according to its typology, should satisfy to be considered TRL8. Technical requirements will be described in D10.3 expected to be delivered on September 2018. Once both operational and technical requirements will be defined, a formal procedure to assess the service TRL will be defined as part of the process to onboard services in the EOSC-hub catalogue.