Operation handbook for EOSC service providers

Abstract:

The EOSC-hub project operates many of the core elements of the European Open Science Cloud, and acts as the main facilitator of onboarding new providers in EOSC through the EOSC Portal. This handbook provides practical information to providers about their responsibilities after they registered their services in the EOSC Portal. The document provides guidance on how to handle user access requests in the EOSC Marketplace, how to respond to EOSC user helpdesk tickets, how to react to and stay informed about security incidents, how to collect user feedback, where to raise issues about EOSC elements to other stakeholders, how to ensure customer-centric service delivery, and how to keep service profiles up-to-date in EOSC. The handbook aims to support service providers operating professionally in the EOSC context.

Digital Object Identifier:

10.5281/zenodo.4068180

Version (date of last update):

6/Oct/2020

Authors:

Gergely Sipos (EGI Foundation), Debora Testi (CINECA), Nadia Tonello (BSC), David Kelsey (STFC), Matthew Viljoen (EGI Foundation), Agnieszka Pułapa (CYFRONET), Owen Appleton (EGI Foundation)

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.

TERMINOLOGY

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

Contents

1. Introduction

Over the past years, numerous policy makers from around the world have articulated a clear and consistent vision of global Open Science as a driver for enabling a new paradigm of transparent, data-driven science as well as accelerating innovation. In Europe, this vision is being realised through an ambitious programme under the heading of the European Open Science Cloud (EOSC). The EOSC initiative has been proposed in 2016 by the European Commission as part of the European Cloud Initiative to build a competitive data and knowledge economy in Europe.

The EOSC will offer 1.7 million European researchers and 70 million professionals in science, technology, the humanities and social sciences a virtual environment with open and seamless services for storage, management, analysis and re-use of research data, across borders and scientific disciplines by federating existing scientific data infrastructures, currently dispersed across disciplines and the EU Member States. The European Commission is providing financial support to implement the EOSC by means of projects under the EU Framework Programme for Research and Innovation (Horizon 2020). The number of Horizon 2020 projects contributing to EOSC reached over 40 by 2020[1] . EOSC-hub is one of the EOSC contributing Horizon 2020 projects. EOSC-hub plays a central role in the EOSC landscape:

- It has defined, developed and runs the central services of EOSC, such as the EOSC Portal[2], a user Authentication and Authorization system as well as a central helpdesk and other critical services.
- It provides 'service onboarding' in EOSC, i.e. provides the tools and process for registering new services in EOSC via the EOSC Portal, and provides the team that validates then publishes the new services online.
- It delivers over 50 generic services (such as compute, storage, data management) and scientific discipline specific thematic services via the EOSC Portal.

EOSC-hub started in 2018 for 3 years to bring together multiple service providers to create “the Hub”, a single contact point for European researchers and innovators to discover, access, use and reuse a broad spectrum of resources for advanced data-driven research. This Hub grew into the initial version of EOSC in 2018, with the official opening of the EOSC Portal in November 2018. Over 270 services have been onboarded to EOSC since 2018.

This handbook provides practical information to providers about their role and responsibilities after they registered their services in EOSC. The document provides guidance on how to handle user access requests in the EOSC Marketplace (section 2), how to respond to EOSC users' helpdesk tickets (section 3), how to react to and stay informed about security incidents (section 4), how to collect user feedback (section 5), where to raise issues about EOSC elements to other stakeholders (section 6), how to ensure customer-centric service delivery (section 7), and how to keep service profiles up-to-date in EOSC (section 8). The handbook aims to support service providers operating professionally in the EOSC context.

---

[1] EOSC Projects: https://eosc-portal.eu/about/eosc-projects

[2] EOSC Portal: https://eosc-portal.eu/

2. Managing service orders

One of the main purposes of the EOSC Portal (https://www.eosc-portal.eu/) is to streamline user access to a diverse set of services and resources that are made available for Open Science. In doing this, the Portal aims to facilitate interdisciplinary and cross-disciplinary workflows that span across resources and services of multiple providers. Open science is not equal to open access and many of the services and resources that are (and will be) federated to EOSC require access control for the users. For example, services that are operated in high-performance compute centres, or databases that serve sensitive data for scientists.

EOSC-hub established an access control system as part of the EOSC Portal, more specifically as part of the Marketplace (https://marketplace.eosc-portal.eu/) component of the Portal. When a new service is registered in the EOSC Portal (and therefore also in the EOSC Marketplace), the provider of the service has to choose the desired integration level with this access control system (also called order management system). The following three options are available for choice:

1. Open access service: The service that is brought into EOSC **does not require users to request access** to the service, because the service is not exposing/using any protected/limited resource therefore any access control would only limit usability. Open access databases (with non-sensitive data), application gateways working with small compute capacity are examples of such services. Although such services sometimes require users to login before using the service, login is only used for traceability reasons and access is automatically granted by the service for the users.
2. Orderable via the custom channel of the service provider: EOSC users need to request access to the service but this **access will be handled through the provider's own access management interfaces and system**. In this case the EOSC Portal has to simply redirect the user to the service homepage where interfaces are offered to request access. Because the access management in this case happens outside the EOSC Portal such services can hardly be integrated into cross-provider workflows and EOSC cannot reach its full potential if many providers go for this option.
3. Orderable via the EOSC order management system: EOSC **users need to request access to the service and can do this through the EOSC order management system.** The provider in this case receives and can react to the access management request through the interfaces offered by the EOSC Marketplace. Services that work at this level can easily be part of cross-provider workflows because the Marketplace can handle together the access requests of all the services/resources that are required for the workflow. EOSC can reach its full potential with providers integrated at this level into the access control system.

The reminder of this section deals specifically with the services that fall into the 3rd category, because for those services the providers have responsibility for responding to user access requests in the EOSC Marketplace system.

Within the EOSC Marketplace, using a ‘webshop’ type interface, EOSC users can request access to multiple services in a single transaction. The access requests are received by the centrally operated Service Order management team of EOSC-hub. This order management team, relying on ‘shifters’, reviews the requests and ensures that only correct and consistent requests are forwarded to the service providers. The EOSC-hub Service Order management team removes spams, and goes back to those users for clarification who submit incomplete or incorrect access requests (e.g. a lot of services are requested, suspicious combinations of services are requested). Correct requests are forwarded to the providers through the "Service Order Target" email addresses that they registered when their services were onboarded in the EOSC Portal. Such an email contains a link to the order management system where the provider can:

- Review details of the access request including the contact information of the user making the request;
- Exchange messages with the EOSC-hub Order Management team;
- Approve or reject the request so that the Order management team can consequently update the status of the request (also visible for the user in the EOSC portal).

At the time of writing there is no time limit for the service providers to respond to access requests. However it is obvious that the response time should be kept minimal for good user experience, especially at this early stage of EOSC.

Specific details on how to log in into the system, and on the request format are available at https://wiki.eosc-hub.eu/display/EOSC/Service+Order+Management+Back+Office+(SOMBO).

3. Responding to helpdesk requests

The EOSC-hub Helpdesk (https://helpdesk.eosc-hub.eu/) is the entry point and ticketing system/request tracker for issues concerning EOSC services. It connects EOSC users and providers via a centrally managed ticketing system that can also federate provider-specific, 3rd party ticketing systems.

Services Providers can choose from three possible levels of integration with the Helpdesk. The level is chosen by the provider as part of onboarding to the EOSC Portal:

1. **Opting out from the Helpdesk:** The provider does not want to participate in the helpdesk and therefore will not be able to receive tickets and notifications from the system. Users will have to reach such providers via other mechanisms, for example by finding them through their service websites, or through the 'Ask a question about this service' form of the EOSC Marketplace. (Such a form exists in the profile of every registered service.)
2. **Direct usage:** The provider wants to reply to service specific tickets in the EOSC Helpdesk. This is the typical choice for services that do not have any existing support helpdesk yet and want to have a more traceable way of managing user requests and responses. If this option is chosen then a service-specific support unit is established within the helpdesk, and the provider can delegate persons to this support unit. When a new ticket is assigned to the unit (either directly by a user, or by the EOSC-hub first line support), then the support persons will be notified in email, and can login to the helpdesk to respond to the ticket submitter.
3. **Email forwarding:** The provider already has an existing ticketing system and would like to receive the EOSC-related user tickets there too. This integration option can ensure that the EOSC tickets are forwarded to the existing ticketing system through an email address. The

provider will receive notification from this existing ticketing system and will have to react to the ticket there too. The EOSC Helpdesk will act only as an incoming channel for new tickets.

Technical details for the service integration can be found in https://wiki.eosc-hub.eu/display/EOSC/Helpdesk.

Whichever level of integration is chosen, the provider is responsible for the timely response of tickets that are assigned to the service in scope. In case of ‘Direct usage’ of the EOSC Helpdesk (2nd option above) service delegates can join the service-specific support unit after registering at https://helpdesk.eosc-hub.eu/. ("Support Staff" menu). After the new role is approved by the responsible member of the support unit, the new member will be able to see and respond to tickets that are assigned to that unit. Members of a support unit are typically subscribed to a single email address which is used by the Helpdesk to send notifications about new tickets and ticket updates (helping the whole team being up-to-date with user support).

The guide to handle a ticket and the description of the ticketing system can be found in the https://wiki.eosc-hub.eu/display/EOSC/Helpdesk.

4. Responding to security incidents

If you, the provider of a service registered in the EOSC Portal Hub Portfolio, are informed of, or discover or suspect a security incident affecting your service, you should inform the EOSC-hub security team without delay, in addition to satisfying any escalation procedure you may also have within your local organization.

To contact the EOSC-hub security teams (there are two collaborating teams - see below for more details) you should send an email to abuse@eosc-portal.eu.

As part of the security incident resolution process, Service Providers are expected to produce the following information:

- Who/how detected or reported the incident
- Host(s) affected (ex: compromised hosts, hosts running suspicious user code)
- Evidence of the compromise, including timestamps (ex: suspicious files, log entry or network activity)
- The actions taken to resolve the incident
- When applicable/available:
    - Possibly affected credential of the user(s), operator(s), consumer(s)
    - Host(s) used as a local entry point to the Service Provider
    - Remote IP address(es) of the attacker
    - What was lost, details of the attack
    - Any remote IP you suspect to be affected
    - Vulnerabilities possibly exploited by the attacker
    - Details of malicious payloads

This information does not all need to be included in the first email. It is best if the initial email is sent as soon as possible containing the information collected so far. The responding security team can then help you form a plan of action and help you to protect your service and its data and help you preserve forensic information.

The CSIRT responding to your report will assist you in all phases of the Incident Response procedure, including the containment, analysis/understanding and recovery phases.

The aim is to minimise the impact of the security incident, to encourage post-mortem analysis and to promote cooperation between Service Providers and Infrastructures. An incident report in a standardized format should be produced during the post-mortem analysis to provide feedback and lessons learned for risk management, to support continuous improvements of security controls to mitigate risks. The post-mortem analysis should reflect on how to apply good security practices, such as access controls, monitoring, applying security patches and hardened configurations. The incident report (a redacted version to remove confidential information) may be shared with other relevant service providers that could be affected by similar incidents.

Do not worry if you do not possess the technical expertise to perform full forensic analysis of the incident. The security teams will advise and help wherever possible.

From time to time the security team may ask you for more details of the incident and you are asked to respond to these requests promptly. Any information you provide will be treated as confidential and will only be transferred to others with your permission.

In other circumstances, EOSC security teams may notice the security incident before you do (or be informed by some third party of suspicious behaviour of your service). In this case you will be contacted by email by one or both of the security teams asking you for assistance as described in the EOSC-hub ISM1 procedure mentioned above. The email will make it clear what action you need to take or what information you need to provide. The security teams ask for your prompt response and collaboration.

5. Gathering user feedback

EOSC does not demand any provider to gather feedback from its users (either from their EOSC users or from users reaching the service outside EOSC). However, it is a good practice for any provider to regularly collect feedback from its users/customers, and and to generally manage relationships with the users/customers using robust and scalable processes.

Because EOSC is typically not the only channel for users to reach a certain service, the user feedback collection and analysis should be carried out outside the EOSC context, covering the EOSC users as well as users who make use of the service via non-EOSC channels.

The FitSM standard (the IT Service Management Standard used by EOSC-hub core services) provides specific requirements[3] on Customer Relationship Management (CRM). Full compliance with FitSM CRM requires the service provider to

- Identify its customers.

---

[3] FitSM-1 - Requirements: https://www.fitsm.eu/download/295/

- Assign a contact person for each of its customers who is responsible for managing the customer relationship and customer satisfaction.
- Establish a communication channel with each customer.
- Carry out service reviews with the customers at planned intervals.
- Be open and manage complaints from customers.
- Manage the satisfaction (feedback) collected from the customers.

If the service requires the users to authenticate, then communication channels can be quite easily established because the user profiles typically include email address or other contact details. Feedback, improvement suggestions can be gathered for example with an online survey (e.g. X days after the first use of the service), or with an online interview (i.e. arranging a teleconference session X days after the first use).

If the service is open access without authentication, then reaching the users is more difficult, but possible with e.g. short pop-up surveys that come up for every user within the service itself.

The collected feedback and improvement suggestions should be fed into the continuous improvement cycle of the service, and if they concern EOSC itself, then should be forwarded to the EOSC-hub Helpdesk (https://helpdesk.eosc-hub.eu/).

6. Reporting & information sharing

6.1 Where to report issues

Issues within the service itself is the responsibility of the service provider. However if the delivery of the service in EOSC fails because of issues in the EOSC framework, then such things can be raised by the provider through the EOSC-hub Helpdesk: https://helpdesk.eosc-hub.eu/. The distributed support team behind the helpdesk will channel the ticket to the appropriate team within the ecosystem.

6.2 Service providers forum

The Service Providers Forum (SPF) has been set up as a means to facilitate communication between EOSC-hub and the Service Providers (SPs). It exists as a mailing list (sp-forum@eosc-hub.eu) and additionally meets during project conferences or other relevant events. The SPF recognises the fact that SPs are a fundamental stakeholder of EOSC and is designed to cater for bi-directional communication between the EOSC-hub project and SPs. The SPF is populated by manually adding the contact email addresses that the SPs provide when onboarding their services. It is worth noting however that the SPF is an open forum, anyone can join SPF events, including SPs interesting to learn more about EOSC prior to onboarding.

Project-based communication that the SPF is used to disseminate to SPs includes: awareness, training, integration and support of EOSC Hub services as well as information and dissemination of project news, major operational news, security related news and upcoming events.

The SPF is used to collect information from SPs including generic feedback of the project - both directly from the users and indirectly from the SP users as well as requirements collection.

6.3 EOSC events, EOSC Liaison Platform

The main EOSC stakeholders are organising various types of events that are useful for service providers to attend and to contribute to. These events are advertised on the EOSC Portal (under the Media menu).

The EOSCsecretriat.eu project operates the EOSC Liaison Platform (https://www.eoscsecretariat.eu/eosc-liaison-platform), an online discussion environment that allows the collection of input and provision of feedback to EOSC governance bodies. Service providers are advised to subscribe for updates on the platform to receive news in areas of their interest.

7. Customer-centric service delivery

7.1 Introduction to the EOSC-hub Service Management System

As part of the EOSC-hub contribution to EOSC, the project is developing and operating an IT Service Management system (SMS)[4]. The SMS ensures a robust and resilient service delivery in the EOSC federated infrastructure with different types of many-to-many relationships between users, providers and clients. The SMS is used by the core elements of EOSC, but the approaches applied there can be a useful for any EOSC provider who wants to ensure professional and customer-centric delivery of its services.

What is IT Service Management?

The key idea behind IT service management could be summarized like this: By following a service-oriented approach, an IT organisation (which may be everything from an internal IT department over a shared IT unit up to an external IT provider) is able to better understand what they do and offer, and how this is aligned to the needs of their customers and users. IT service management (ITSM) refers to the entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to design, plan, deliver, operate and control information technology (IT) services offered to customers. And by implementing IT service management processes, the activities carried out to plan, deliver, operate and control these services become more structured and repeatable, with clearly defined responsibilities. All this helps an IT organisation to increase their level of professionalism and organisational maturity.

---

[4] https://www.eosc-hub.eu/eosc-hub-key-exploitable-results/#KER2

The EOSC-hub SMS represents the entirety of activities performed by the providers that contribute to the EOSC core to plan, deliver, operate and control the services offered to EOSC. The SMS also covers (to different extent) the activities of those service providers that have been onboarded to EOSC via the EOSC Portal.

The activities carried out in the context of the SMS are structured and organised into processes and procedures according to the FitSM IT Management standard[5]. FitSM is a free, pragmatic, lightweight and achievable standard aimed at facilitating service management in IT service provision, including federated scenarios. By defining requirements, the 14 processes of FitSM help service providers:

Process	Objective
Service portfolio management (SPM)	To define and maintain a service portfolio
Service level management (SLM)	To maintain a service catalogue, and to 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 suppliers
Service reporting management (SRM)	To specify all service reports and ensure they are produced according to specifications in a timely manner to support decision-making
Service availability and continuity management (SACM)	To ensure sufficient service availability to meet agreed requirements and adequate service continuity
Capacity management (CAPM)	To ensure sufficient capacities are provided to meet agreed service capacity and performance requirements
Information security management (ISM)	To manage information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information are preserved
Customer relationship management (CRM)	To establish and maintain a good relationship with customers receiving services
Supplier relationship management (SUPPM)	To establish and maintain a healthy relationship with suppliers supporting the service provider in delivering services to customers, and monitor their performance
Incident and service request management (ISRM)	To restore normal / agreed service operation within the agreed time after the occurrence of an incident, and to respond to user service requests
Problem management (PM)	To investigate the root causes of (recurring) incidents in order to avoid future recurrence of incidents by resolving the underlying cause, or to ensure workarounds/temporary fixes are available
Configuration management (CONFM)	To provide and maintain a logical model of all configuration items (CIs) and their relationships and dependencies

---

[5] FitSM IT Service Management standard: https://www.fitsm.eu/

Change management (CHM)	To ensure changes to CIs are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services
Release and deployment management (RDM)	To bundle changes of one or more CIs to releases, so that these changes can be tested and deployed to the live environment together
Continual service improvement management (CSI)	To identify, prioritize, plan, implement and review improvements to services and service management

For each of these processes, as well as for a number of general aspects in the context of ITSM, FitSM (within the FitSM-1 document[6]) defines implementation requirements (approx 5 per process), while the FitSM-2 document[7] provides guidelines on the activities to set up and implement ITSM using these processes. The FitSM-3 document[8] describes the proposed roles to be assigned to execute the ITSM processes as part of a service management system.

7.2 Integration with the EOSC-hub SMS

At a base level, all onboarded services become in the scope of EOSC-hub SPM when they are included into the EOSC Service Portfolio, and then publicly exposed in a Service Catalogue (the EOSC Portal and its Marketplace - See Section 2 earlier). How the scope of other EOSC-hub SMS processes impacts on new onboarded services depends on the choices the service providers make for integrating with other Hub Portfolio components (those that are described in Section 3). For example, enabling ‘ordering’ (i.e. users have to request access to the service via the EOSC Marketplace) will bring the onboarded service partially into the scope of CRM; using the Helpdesk involves the onboarded service in the ISRM process; etc. Additional integration activities may bring the services within the scope of other SMS processes.

Some examples will help to further illustrate this approach:

- Suppose that an onboarded external service wishes to make use of the EOSC hub Helpdesk service (Section 3.4). This requires you to provide a second line support entity, either with the helpdesk that You may already be using, or integrated with the EOSC-hub Helpdesk service. In both options Your support team will be expected to reply to the incidents in a timely manner according to the agreed timeline. These timelines are defined according to the Incident and Service Request Management (ISRM) process of the EOSC-hub SMS.
- Suppose now that an onboarded service wants to make use of an EOSC Authentication and Authorization Infrastructure (Section 3.1) to aid its users with single sign on functionality. This requires the provider to meet minimum security requirements (e.g. responsive security contact; channel for alerts about security incidents) and to accept the EOSC hub standard site security policy in order to ensure the secure exchange and processing of attributes of

---

[6] FitSM-1 document - Requirements: https://www.fitsm.eu/downloads
[7] FitSM-2 document - Objectives and Activities: https://www.fitsm.eu/downloads
[8] FitSM-3 document - Role model: https://www.fitsm.eu/downloads

end users by the AAI. These requirements are defined in the Information security management (ISM) process of the EOSC-hub SMS.

7.3 Where to ask assistance

FitSM is and will remain free for everybody. This covers all parts of the standard, including the core documents (FitSM-0, -1, -2 and -3), the templates and samples (FitSM-4), the guides (FitSM-5) as well as the FitSM maturity assessment tool (FitSM-6) - all available at https://www.fitsm.eu/downloads/.

During EOSC-hub EGI offers training about FitSM to EOSC-hub member institutes. These trainings are organised at EOSC-hub events, and from Q3 of 2020 EGI is conducting them remotely. EGI also provides consultancy for those who wish to implement FitSM within their organisation. Please contact the team via the FitSM entry in the EOSC Marketplace: https://marketplace.eosc-portal.eu/services/fitsm.

8. Changing your 'EOSC configuration'

Should you want to change the description of your service in the EOSC Portal/Marketplace, or should you need to do any other configuration changes to your service in the EOSC context, please ask for this in the EOSC-hub Helpdesk (https://helpdesk.eosc-hub.eu/).

9. Future outlook

The EOSC-hub project mobilised providers from the EGI Federation[9], EUDAT CDI[10], INDIGO-DataCloud[11] and over 20 major European research infrastructures and communities. These providers have contributed to the EOSC Portal & Marketplace, and are delivering a rich set of services through these services, which will continue to be operated after the end of EOSC-hub.

A Horizon2020 call, titled '*INFRAEOSC-03-2020 Integration and consolidation of the existing pan-European access mechanism to public research infrastructures and commercial services through the EOSC Portal*'[12] closed on June 18, 2020. The project to be funded in this call will operate and further develop the EOSC Core, including those elements that are covered in this document. The project is expected to start in 2021 and run for 30 months.

Another project, called EOSC Enhance[13] started at the end of 2019 to increase the functionality of the EOSC portal. The project is implementing interfaces for EOSC service providers to allow self-management of service profiles within the EOSC Portal and Marketplace. This new system is expected to be published towards the end of 2020 and will simplify the way service profiles can be maintained and presented for EOSC users.

---

[9] http://egi.eu/

[10] http://eudat.eu/

[11] https://www.indigo-datacloud.eu/

[12] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/infraeosc-03-2020

[13] https://www.eosc-portal.eu/enhance