D7.1

EOSC Service Planning

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

Version 1
September 2021

D7.1 / EOSC Service Planning

Lead by **EGI Foundation**
Edited by Matthew Viljoen (EGI Foundation)
Reviewed by Luciano Gaido (INFN) and Rocío Mantero Cejudo (Lifewatch)

Dissemination level of the document

Public

Abstract

This deliverable covers the gap analysis of the EOSC Service Management System (SMS) supporting the planning, development, maintenance, and delivery of the EOSC Portal and EOSC-Core services, and to a lesser extent the EOSC-Exchange services. It examines the state of the existing relevant work at the start of the EOSC Future project in reference to previous projects (e.g. the EOSC SMS as developed within the EOSC-Hub project) and identifies areas needed for improvement in the light of the evolving EOSC landscape for which the EOSC Future project is designed to cater. Emphasis is given on the operational aspects of service delivery behind the EOSC Portal and EOSC-Core services, although aspects of the EOSC-Exchange are also considered.

Version History

Version	Date	Authors	Description
V0.1-0.6	29/07/2021	M Viljoen (EGI Foundation) et al.	First version incorporating feedback from QRP1 review and converted to correct Word format
V0.7	03/08/2021	M Viljoen (EGI Foundation)	Incorporating feedback from QRP2 review
V0.8	10/08/2021	M Viljoen (EGI Foundation)	Application of correct template
V0.9	26/08/2021-13/09/2021	M Viljoen (EGI Foundation)	Document finalization, incorporating minor comments and circulation of final document before submission
V1.0	17/09/2021	M Viljoen (EGI Foundation), Ron Dekker (TGB), Mike Chatzopoulos (ATHENA)	Submission to EC by PC (ATHENA)

Copyright Notice

Table of Contents

Table of Figures

List of Abbreviations

Acronym	Definition
AAI	Authentication and Authorization Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
AEGIS	ARC Engagement Group for Infrastructure
CAB	Change Advisory Board
CAPM	Capacity Management
CHM	Change Management
CI	Configuration Item
CSIRT	Computer Security Incident Response Team
CONFM	Configuration Management
CMDB	Configuration Management Database
CSI	Continual Service Improvement
EOSC	European Open Science Cloud
EPOT	EOSC Portal Onboarding Team
FAIR	Findability, Accessibility, Interoperability, Reusability
FAQ	Frequently Asked Questions
FIM4R	Federated Identity Management for Research
FitSM	Standards family for lightweight IT Service Management
ICT	Information and Communications Technology
IGTF	International Grid Trust Federation
IoC	Indicators of Compromise
ISM	Information Security Management
ISRM	Incident and Service Request Management
KEDB	Known Error Database
OLA	Operational Level Agreement
PM	Problem Management
RDM	Release and Deployment Management
REFEDS	Research and Education Identity Federations
R&E	Research and Education
RfC	Request for Change
RoP	Rules of Participation
MVE	Minimum Value EOSC
SACM	Service Availability and Continuity Management
SCI	Security for Collaboration among Infrastructure
SDTP	Service Design and Transition Package
Sirfti	Security Incident Response Trust framework for Federated Identity

SLA	Service Level Agreement
SLM	Service Level Management
SMS	Service Management System
SFRM	Supplier Federation member Relationship Management
SOCRM	Service Ordering and Customer Relationship Management
SPM	Service Portfolio Management
SQA	Software Quality Assurance
SQAaaS	SQA as a Service
SRM	Service Reporting Management
TCB	Technical Collaboration Board
UA	Underpinning Agreement
WISE	Wise Information Security for E-infrastructures
WP	Work Package

1 Introduction

1.1 Services

There are currently two portfolios in existence within EOSC, services within the EOSC-Core (services and resources necessary for implementing EOSC as a federated system) and those within the EOSC-Exchange (services and resources onboarded from Research Infrastructures and private companies including thematic and generic services and compute/storage resources).

The EOSC Service Management System (SMS) is primarily intended for the services within the EOSC-Core to facilitate a consistent and high-quality service delivery. However, there are aspects of the EOSC SMS that also include resources within the EOSC-Exchange - for example Service Portfolio Management (SPM) includes onboarded resources and procedures for onboarding. Other processes such as Service Level Management (SLM), Incident and Service Request Management (ISRM) and Information Security Management (ISM) all support the EOSC-Exchange in addition to the EOSC-Core.

Services within the EOSC-Core have been defined within the EOSC Future project description of activities to include the following functions:

- Registry of services
- Marketplace
- Monitoring
- Helpdesk
- Accounting
- EOSC Portal frontend
- Open Science Monitor
- Data Usage Statistics
- Authentication and Authorization Infrastructure (AAI)

The development of the EOSC SMS within EOSC Future will ensure that the SMS is suitable for the full production delivery of services meeting these functions as well as supporting the onboarding, central discovery and ordering of external resources within the EOSC-Exchange.

This deliverable includes an examination of the SMS status at the start of the project along with the expected development work to bring the SMS to a complete fit-for-purpose SMS which caters for the expected scale of EOSC at the end of the project. It should be noted that the EOSC landscape has developed at an accelerated pace since EOSC was first conceived. It has also changed direction, e.g. the introduction of the 'EOSC Portal' concept during the EOSC projects prior to EOSC Future. The SMS needs to adapt 'in flight' to such unexpected changes - it is likely that this will be the case during EOSC Future. As such, the initial assessment of the work within the SMS as presented within this deliverable is likely to evolve.

The EOSC SMS within EOSC Future project is built on the prototypal SMS developed within the EOSC-Hub project, which was built around the FitSM standards family[27]. Within the EOSC Future proposal, no standard, standards family, or framework was specified for the SMS. Therefore, the original EOSC-Hub SMS will be developed according to needs incorporating FitSM and other standards or frameworks within the SMS as necessary, taking into consideration the background and experiences of different partners within the project who may have first-hand knowledge of different SMS standards or frameworks.

Despite what was originally intended in the EOSC Future Description of Activities text for this deliverable, a gap analysis of the individual EOSC-Core technical services themselves is out of scope. WP7 does not include effort in developing the EOSC-Core services but delivers the services and the Service Management System covering all aspects of service delivery as well as the maintenance and support of these services. The design and implementation of the EOSC Portal back office, including the delivery of software for the EOSC-Core, is performed within WP4. As such it is considered that a 'gap' analysis of the technical services themselves would be more appropriate to be covered within WP4; in particular Deliverable **D4.1 'Back-Office design, functional and technical specifications'** and **D4.2 'Back-Office Requirement Analysis'** as well as within **D7.3 'EOSC Federated Authorisation and Authentication Activities'**.

Figure 1.1 below shows the parts of the project relevant to the SMS and the components of the SMS being developed within the project, along with the principal relations between them. If all relations were shown, this diagram would become too complex. It is also likely that further relations will become apparent during the continuing maintenance and development of the SMS over the duration of the project. It is noted that the acronyms signifying SMS process names within this figure are described within the different sections of this deliverable.

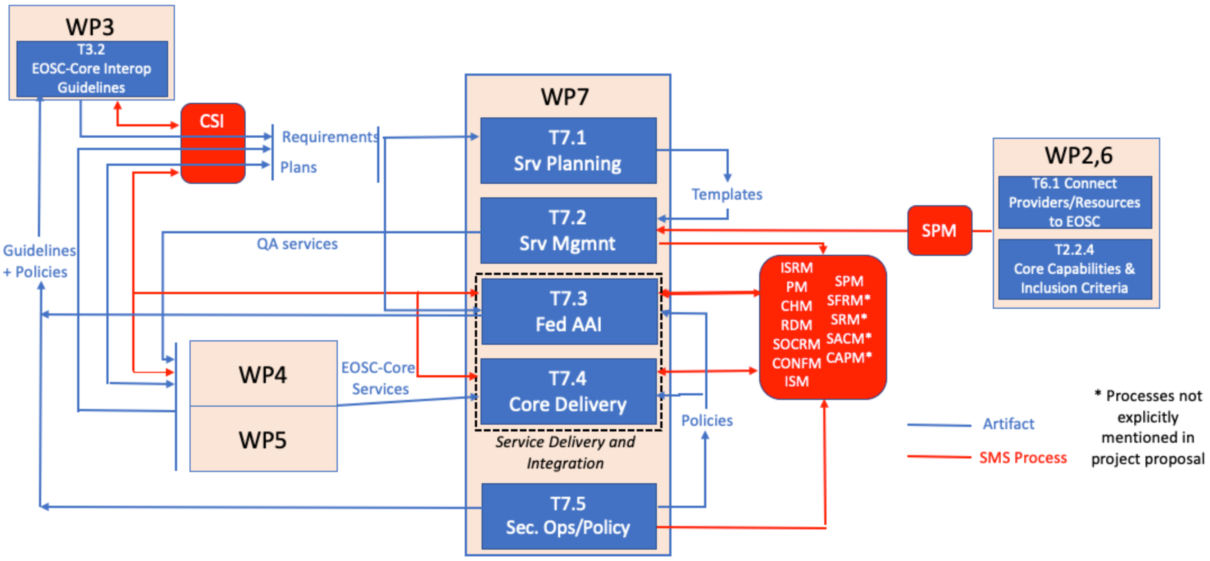

Figure 1.1: SMS Components and Interfaces

1.2 Sustainability Considerations of the EOSC SMS and its Supporting Services

The EOSC SMS is designed to support all aspects of delivering and managing EOSC Services. As the EOSC becomes more established, continuity of the EOSC services becomes essential, and the transition from one project to another sustaining the services and their service delivery should be as seamless as possible to the users. This implies that the SMS and the services supporting it (e.g. internal ticket handling system, service onboarding and ordering) need to be continued without interruption, regardless of who is running the services and the project-specific aspects of the SMS itself. This includes project branding of services, e.g. at the Domain Name Service level of dependent services such as Confluence and Jira, as well as mailing lists such as those for onboarding and security. At the beginning of the EOSC Future project and until the proper coordination with previous projects was achieved there was a negative impact to several EOSC-Core services such as onboarding and service ordering as a result. This is an important lesson learnt that must be prevented from happening again at the end of the EOSC Future project and subsequent projects supporting EOSC, by taking actions early enough for the sustainability of EOSC SMS.

This aspect will be the subject of further discussion during the project implementation, but one potential solution would be to completely disconnect the hosting of the EOSC SMS and its supporting services from time-limited projects and project branding, as well as a completely disconnect the SMS and its supporting services from any partner. The delivery of the EOSC SMS and its supporting services could potentially be covered by an OLA with the EOSC Association for a fixed duration which could correspond to the lifetime of projects sustaining and further developing EOSC.

2 Service Planning and Delivery

2.1 Service Portfolio Management

Service Portfolio Management (SPM) within EOSC Future (and indeed EOSC) has a dual role. The generic objective of SPM is to define and manage a service portfolio, but this is divided into:

- For **the EOSC-Core Platform services**, which enable the operation of an EOSC Federation, to define and manage a service portfolio, to ensure that the EOSC-Core Platform supports effective operation of EOSC-Core and supports the EOSC-Exchange. The scope resembles a more traditional view of Service Portfolio Management in IT Service Management. Within the EOSC Future project this work occurs in Wp2 Task 2.2. involving the developers and operators in the technical work packages.
- For **the EOSC-Exchange services**, the scope is rather unusual in terms of a traditional SMS. EOSC Future, and in future EOSC as personified by the EOSC Association is not the owner of these services, rather it exposes them to customers, while trying to bring some level of cohesion to them, and work to increase the coherency, maturity, interoperability, and composability. This is done through collecting providers and resources and onboarding them through WP6 Task 6.1, taking input from Wp3 Task 3.2 on the EOSC Profiles, Wp2 Task 2.2. on inclusion criteria and other inputs from the technical work packages.

SPM for the EOSC-Core thus needs to ensure that services meet identified needs and has identified capabilities to support EOSC-Core operations. On the other hand, SPM for EOSC-Exchange is not about selecting the best services for EOSC to expose to researchers, but about providing support and quality standards to ensure a rich variety of services exist in the EOSC-Exchange from which researchers can select and combine.

2.1.1 Status at the beginning of the project

SPM for EOSC-Exchange began in a relatively developed state as it was not a 'from scratch' effort. The current process is shown in Figure 2.1.

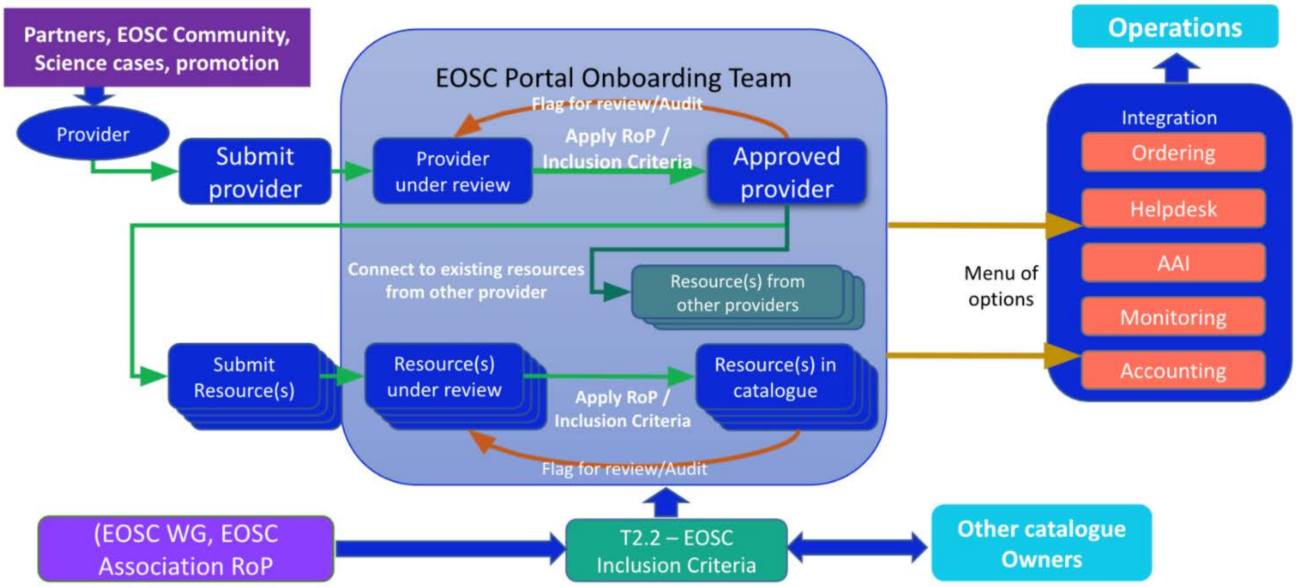
Partners, EOSC Community, Science cases, promotion
Provider
Submit provider
EOSC Portal Onboarding Team
Flag for review/Audit
Provider under review
Apply RoP / Inclusion Criteria
Approved provider
Connect to existing resources from other provider
Resource(s) from other providers
Submit Resource(s)
Resource(s) under review
Apply RoP / Inclusion Criteria
Resource(s) in catalogue
Flag for review/Audit
Operations
Integration
Ordering
Helpdesk
AAI
Monitoring
Accounting
Menu of options
(EOSC WG, EOSC Association RoP
T2.2 – EOSC Inclusion Criteria
Other catalogue Owners

Figure 2.1: EOSC Onboarding process to EOSC-Exchange

The process was developed in detail as part of the EOSC SMS under EOSC-Hub, and a significant portion of the work also crosses over with EOSC Enhance, which overlaps both EOSC-hub and EOSC Future and helped by providing continuity of such effort. Several of the most complex tasks around SPM were tackled during the integration between the EOSC-hub and eInfraCentral[1] catalogues, and EOSC Future inherited basic procedures for onboarding, written jointly by the EOSC Enhance and EOSC-hub projects. The process is multistage but accommodates a range of use cases from onboarding single services, to simultaneously onboarding large sets of services via APIs, or to transfer provider and resource records from other cooperating catalogues (which is currently being tested together with some of the Regional EOSC projects). This work is currently undertaken by the EOSC Portal Onboarding Team (EPOT) which builds on work previous done by EOS-hub, EOSC Enhance and other projects with catalogues or contributing to onboarding.

For EOSC-Core SPM, is slightly more complex. The current set of EOSC-Core functionalities offered by EOSC Future are those developed in WP4 and WP5, and the selection of them was conducted through the proposal preparation process rather than a traditional SPM process. Currently, through task WP2 Task2.2, the capabilities of the proposed EOSC-Core services must be assessed versus the expected capabilities for EOSC-Core set out in the EOSC Architecture Working Group view on the Minimum Viable EOSC [1]. This must be mapped to the technical services available, and their integration and evolution aligned to these needs, as well as with input from the EOSC Association and wider EOSC stakeholder communities.

2.1.2 Areas for improvement

For EOSC-Exchange SPM, the priority is bringing new staff into the EPOT activity and training them on onboarding procedures in order to have an effective onboarding team. This goes along with managing the migration from the previous project collaboration tools to those in the EOSC Future project. Following this there is a need to document automation of the process to the greatest extent possible to manage the workload it implies. Significant part of the previous projects' work performed by EPOT members can now be automated, allowing EPOT members to concentrate on the more complex issues requiring human intervention.

Updating the Rules of Participation and Inclusion Criteria is essential, but this needs to be aligned with the newly formed EOSC Association Task Force on Rules of Participation Compliance Monitoring, which is only expected to start being active in September 2021. As a result of this, initial improvements or fixes in this area may be temporary rather than permanent.

One of the most critical issues, however, is how to effectively onboard data into EOSC, which has not been performed in previous projects. For this, various paths have been considered, currently converging not to directly onboard data, but to bringing data into EOSC through EOSC compliant services which expose it, with a specific class of service called a **Data Source** being defined. See Figure 2.2.

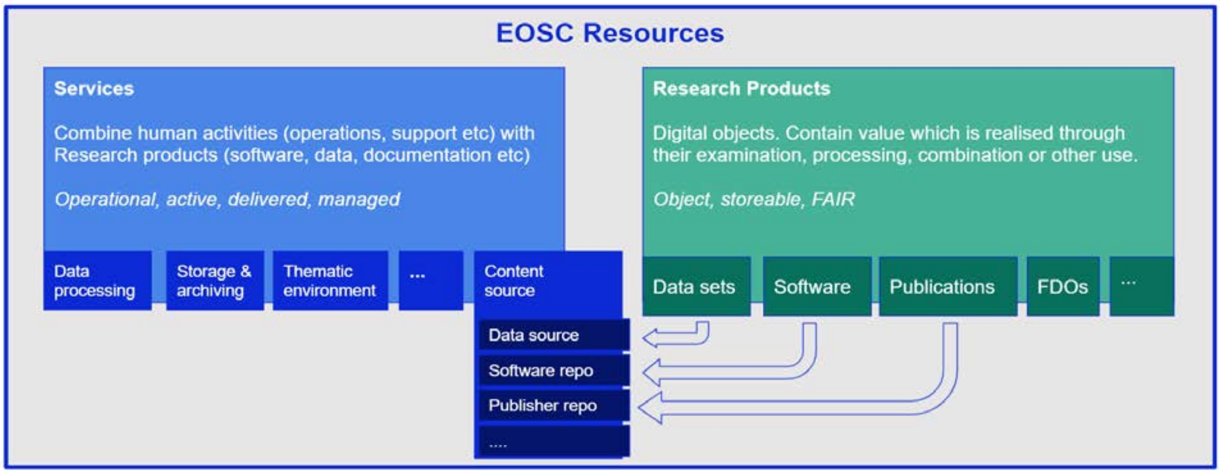
EOSC Resources
Services
Combine human activities (operations, support etc) with Research products (software, data, documentation etc)
Operational, active, delivered, managed
Data processing
Storage & archiving
Thematic environment
...
Content source
Data source
Software repo
Publisher repo
....
Research Products
Digital objects. Contain value which is realised through their examination, processing, combination or other use.
Object, storeable, FAIR
Data sets
Software
Publications
FDOs
...

Figure 2.2: EOSC Resources and path to connect services to data

[1] eInfraCentral prepared an early listing of services in the infrastructure domain which was integrated into EOSC via EOSC Enhance.

For EOSC-Core SPM, the first step is to have a clear mapping of project activities to the Minimum Value EOSC (MVE), and from this to plan how to proceed with the proposed improvements (including a means of onboarding data through a data source). Following this an increased detail on each EOSC-Core service must be created, possibly including a Service Design and Transition Package (SDTP).

2.2 Service Level Management

The purpose of Service Level Management (SLM) is 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 under the scope defined in the SLM Framework.

2.2.1 Status at the beginning of the project

Within the EOSC-hub SMS, the SLM process was defined along with a suggested *Hub Participation Agreement template* for services within the EOSC-hub portfolio, containing the initial services within the EOSC-Core. This *Hub Participation Agreement template* covered aspects such as service hours, support channels and incident handling target times. It also contained service level targets, requirements on service reporting, escalation procedures if these targets were violated. Finally, it contained expectations on the service supplier regarding Information Security and their responsibilities as well as the expectations on the customer side, which was effectively the EOSC-hub project itself.

Procedures were defined within the EOSC-hub SMS supporting the definition and maintenance of the *Hub Participation Agreement template* along with workflows related to it, for example escalation procedures in case of violation.

The *Hub Participation Agreement template* and its associated procedures were however not put into practice as the main reason being that the EOSC-hub Service Validation Board (SVB) which was the body authorised to approve the implementation of this process was, not established until the last year of the project.

2.2.2 Areas for improvement

Reliable service delivery of the EOSC-Core services is fundamental for the success of EOSC Future. It is therefore necessary that the SLM process needs to build upon the initial work done within EOSC-hub and to fully implement an agreement covering the delivery of EOSC-Core services. The agreement needs to be updated to reflect the changes within EOSC Future, the new terminology and updated service delivery expectations. It then needs to be ratified by the EOSC Future project management and governance. At this point it can be properly implemented along with the other processes supporting SLM, for example, Service Reporting Management (SRM), Configuration Management (CONFM), Service Availability and Continuity Management (SACM), Capacity Management (CAPM), Information Security Management (ISM) etc.

Since SRM (along with SPM) are high level processes determining much of the SMS, it is important that this work is completed towards the beginning of the project - a reasonable timeframe would be to have the agreements ratified within the first year.

By the end of the project, all EOSC-Core services should be covered by agreements and related aspects of all supporting processes should be fully implemented and functioning. Monitoring of the services to verify whether target levels are being reached should be established and regularly run within SFRM to support this process. Reports of this monitoring should be produced for all the EOSC-Core services.

2.3 Service Reporting Management

The goal of Service Reporting Management (SRM) is to specify all service reports and process reports, and ensure they are produced according to specifications in a timely manner to support decision-making.

2.3.1 Status at the beginning of the project

Based on the outputs from EOSC-hub, the following documents and processes are currently available:

- The *Hub Participation Agreement[28]*, which includes the SLAs for service delivery, exceptions, helpdesk support, incident handling, service level targets, limitations & constraints, communication, regular reporting, violations, escalation & complaints, information security & data protection, and responsibilities of the internal supplier. There are some gaps in it, however, such as the "quality of support level", as well as each of the categories under communication. This document needs to be reviewed to assess if it is fit for purpose for the EOSC Future project and additional amendments will need to be made because the EOSC Future project engages with service providers directly, instead of engagement with only EGI within the EOSC-hub project.

- The *Service Reports Catalogue[29]*, as well as the *Process Reports Catalogue* which need to be reviewed and revised to define the scope of the work and any new reports that may be required, for example in the areas of capacity management, change control and continuity.

2.3.2 Areas for improvement

The *Hub Participation Agreement* was not possible to be completed within EOSC hub project lifetime due to time restrictions; for EOSC Future, finishing that work would imply significant improvements necessary to be applied. Reports at the process level need to be in scope, as well as those reports related to service level management. It needs to be determined whether the reports are still relevant, and any necessary changes should be implemented. In addition, EOSC Future has no mechanism for monitoring that the reports have been completed. There needs to be some process for ensuring that these are completed and the mechanism necessary for this should be implemented.

Lastly, it would be an objective to complete a similar document, to the *Hub Participation Agreement*, within EOSC Future; this document will be an 'overarching' OLA document due to the fact that such agreements will not directly be with EGI this time, but potentially with the EOSC Association and completed within the timeframe of the EOSC Future project. Within EOSC Future, the agreements should be made with the individual service providers (which provide the EOSC-Core services).

2.4 Service Availability and Continuity Management

The purpose of Service Availability and Continuity Management (SACM) is to ensure that the level of service availability delivered by a service meets the service levels targets agreed on in the OLA and the availability needs in general, and that an adequate level of service continuity is guaranteed in case of exceptional events. The process ensures that the monitoring of the services' availability is adequately done to detect a failure as soon as an incident occurs and then to trigger the Incident and Service Request Management (ISRM) as well as potentially the Problem Management (PM) processes for reporting the incident and for working on its resolution.

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

2.4.1 Status at the beginning of the project

The EOSC-hub SACM process was defined using the EGI SACM process as a starting point and evolved to consider the EOSC-hub needs. The two internal Service Management System audits performed during the EOSC-hub project provided further input to improve the process.

Three procedures were created to:

- Manage an event of a major loss of service.
- Create and maintain Service Availability and Continuity plans
- Verify SACM process of a federated member or supplier providing service in the HUB portfolio

The monitoring of the services under scope during the EOSC-hub project was established and the related Availability and Continuity plans were created, in collaboration with the federated members of the project.

2.4.2 Areas for improvement

The scope of the process is going to be updated to cover (at least) all the EOSC-Core services mentioned in Section 1.1. Other services, belonging to EOSC-Exchange, might be included if a particular need emerges.

Given the updated scope, it will be ensured that all the relevant services are properly monitored, and the related Availability and Continuity plan is created: for the services that were already in scope of the process and that underwent major changes during the transition from EOSC-hub to EOSC Future it might be decided to create an Availability and Continuity plan *ex novo*. During the development of the process under the EOSC-hub project several Availability and Continuity risks were identified, these being a list of risks and threats quite common considering the services that were under scope. It is now necessary to review this list and add any new risk or threat that can be related to the new services included in the scope of the process.

It is not expected to have major changes to the procedures defined so far, even though it might be needed to review the process of gathering Availability and Continuity requirements given the new landscape where the services are delivered.

2.5 Capacity Management

The goal of this process is to ensure that sufficient capacities are provided to meet agreed service levels and performance requirements for services that are part of production services within the EOSC Portfolio. The Capacity Management (CAPM) is usually triggered before the release of a service into the production environment (e.g. during the production of a Service Design and Transition Package, SDTP), with a periodic reiteration during the lifetime of the services in the catalogue: the process considers all resources required to deliver the IT service, and plans for short-, medium-, and long-term business, capacity, and performance requirements.

The result of this analysis is the production of a plan that documents the current level of resource utilisation and service performance and, after consideration of the service strategy and plans to forecast the future requirements for new IT resources, to support the IT services that underpin the business activities. The plan clearly specifies any assumptions made as well as any recommendations quantified in terms of resources required, cost, benefits, impact, etc.

2.5.1 Status at the beginning of the project

The EOSC-hub CAPM process was set-up based on the experience gained with the CAPM process within the EGI SMS and improved during the lifetime of the EOSC-hub project, especially working on the outcomes of the internal audits that occurred during EOSC-hub.

The procedures created within the process handle with the following situations:

- Creation and Approval of a Capacity Plan and the scheduling of regular planned reviews
- Verification of the CAPM process of a federated member or supplier providing service in the HUB portfolio

A template for the Capacity Plans is available[30], along with the criteria to produce them. The Capacity Plans were created for all the services under scope during the EOSC-hub project, in collaboration with the federated members of the project.

2.5.2 Areas for improvement

The scope of the process needs to be updated to include, at least, all the EOSC-Core services. New capacity plans will be created, and the existing ones will be reviewed to assess all the capacity aspects of the services that underwent major changes during the transition from EOSC-hub to EOSC Future, as well as any other significant changes during the EOSC Future.

Taking into consideration the new management structure of EOSC Future, the approval process of a capacity plan should be revised.

2.6 Information Security Management

2.6.1 Status at the beginning of the project

Information security management (ISM) aims to preserve the necessary confidentiality, integrity and availability of what is commonly labelled *'information assets'*. Following the classification model of *'information assets'* developed in EOSC-hub, these assets in the EOSC context are considered at the level of *'services'*, with the service provider designated as the asset owner in the ISM context. This by design includes the EOSC-Core services, but also the security of services and data in the EOSC-Exchange should be considered. By considering services and data as the assets of the EOSC, the security management process emphasises the subsidiarity that – if only because of the sheer scale – must underpin EOSC security: service providers in the EOSC-Exchange are and remain responsible for the security of their services, and they play, and must play, a significant role in keeping the EOSC secure.

While the EOSC ISM policies and procedures are designed to keep the core EOSC components secure and protect the interactions between EOSC participants, providers have an autonomous responsibility to design and operate their services securely, consider the integrity and availability of their own services, and conduct appropriate risk assessments when participating in the EOSC.

Other SMS processes provide the information security management process with its basic inventory of service assets: the EOSC-Core services are explicitly in scope of the SMS, and EOSC-Exchange services are on-boarded and managed through SMS processes and a register of them is maintained. Information Security Management is then concerned with the coordination of security risk assessment, the maintenance of (operational) security policies, planning and deployment of information security controls (in this context also by promoting good-practice controls at the respective service providers, and sharing of threat intelligence), and managing what is politely called *'information security events'*: responding to security incidents and intrusions, and supporting forensics, remediation, and resolution of break-ins. Following the distributed nature of the EOSC, access controls are devolved to each service and service provider, where they can be supported by the EOSC AAI that is being established through EOSC Future as well.

Composition of services within the EOSC ecosystem creates mutual dependencies between service providers, specifically also in managing the attributes of security and trust: integrity, confidentiality, resilience, and availability. In particular, service composition and layering of services increases the administrative *'trust distance'* between service providers, between service providers and users: the desirable proxies and composed services have to be fully engaged in trust policy, risk assessment, and operational security incident response so that miscreants cannot hide within the EOSC ecosystem, masquerading as regular users through compromised credentials, or hiding in services and exposing users and research communities to unexpected threats.

The security and trust domain of the EOSC does not stop at the boundary of the EOSC-Core services, but necessarily extends to the services in the EOSC-Exchange, as well as involving research community services from which the trust in users ultimately flows.

To make the EOSC ecosystem trustworthy and secure, both the EOSC-Core services and the services and content available in the EOSC-Exchange at large must be secure. This is in the interest of not only the end-users (for whom the EOSC should appear as a single and integrated whole) but also of its peer service providers, between which - by design - mutual dependencies exist. Whether on its own or through its interaction with other providers, peers in the EOSC ecosystem should not be exposed to unacceptable risks as a result, since the size and scope of this ecosystem will be changing continuously, and the *'risk of participation'* thus cannot be determined in advance.

As the EOSC ecosystem is being assembled, security policy and operations vary widely across service providers and communities. Whereas there is significant operational security expertise in the (large-scale) infrastructures and service providers, web-scale security expertise cannot be taken for granted for all service providers. Both knowledge and experience are (globally) scarce and highly sought after by many sectors outside the research and academic domains - thus making it harder for many service providers in the research and education sector to attract such personnel. In addition -and at the risk of making overly broad generalisations- the security awareness at many service providers is limited, with functionality and content taking precedence over security controls, engineering for secure coding, and adherence to the evolving baselines and best practices. This may be especially pertinent when the security context changes and services become (rightfully) more exposed and accessible through the EOSC. In the EOSC context, the best opportunity to establish a secure and trustworthy ecosystem is through collaboration and information sharing, complemented by awareness raising, training & exercising. While this insight itself is obviously not new, collaboration and sharing are -until now- mostly contained within the various verticals: a single infrastructure, a country or region, group of service providers deploying a common piece of software. Beyond the relationships established through the EOSC-Hub Information Security Management system, which provides links between e-Infrastructures and a selected number of (technically) highly-organised research infrastructures, there is currently no structural basis for response to incidents involving the EOSC that cross service provider and infrastructure boundaries, and the incorporation of many new service providers in the EOSC will likely only aggravate the sharing complexity unless a framework is put in place, and backed by an effective computer security incident response team ("CSIRT") that can jumpstart the security activities by leveraging existing (personal and community) connections.

But the EOSC is by design a multi-stakeholder and multi-domain environment, bringing challenges in balancing detailed technical remediation intervention with the autonomy and a large amount of heterogeneity in the ecosystem that requires engagement by everyone. A single CSIRT team also cannot be responsible for responding to incidents both in the EOSC-Core and in an indeterminately large number of services in the EOSC-Exchange, just because of its sheer size and complexity. Work within infrastructures themselves, as well as in identity federations (such as the Security Incident Response Trust framework for Federated Identity, *Sirtfi*), have shown that hub-and-spoke structures for response and information sharing, with an expert coordinating centre, work well to contain the spreading of incidents. Leveraging both organisational and personal trust relationships - also outside of the immediate EOSC context, and leveraging trust also with other sectors, national CERTS, and (law enforcement) agencies - is essential for such a team to deal with intrusions.

2.6.2 Areas for improvement

To address these challenges in the EOSC, the risk management, the establishment of a security policy and trust *'baseline'*, training of service and content providers, and operational readiness challenges are considered the foundation layer that must be present as an operational capability. And, since regardless of policy and good practice incidents will happen, a technical core comprising expert forensics and rapid sharing of information and indicators of compromise must be in place and ready to respond – supporting both the EOSC-Core service that constitute the ecosystem's portal as well as supporting the layer of content and service providers connected to it.

A range of actions, proposed in the white paper *Trust Coordination for Research Collaboration in the EOSC era* [2] highlights the challenges at the central, *'portal'* level, and expects responsible participation by the providers connected to it.

Therefore, also each service (and infrastructures delivering research-enabling services) should include its own mechanisms that ensure integrity, availability, and trust for the services offered to the EOSC, as well as integrate with the activities of the EOSC ecosystem. With policy and operational teams specifically attuned to the type of services offered by the infrastructure to the EOSC portal, they alone can provide the technical mechanisms and operational controls to identify, contain, mitigate, and resolve incidents.

In this context, *services* and *user communities* (through their AAI Proxy) are considered as the (conceptual) *assets* of the EOSC as defined in the information security management system. Based on the classification of the services in the EOSC-Exchange and EOSC-Portal operational readiness level, available impact metrics for the service, utilisation, and interconnections with other services - it will be subsequently derived how, and to what extent, each of the ISM procedures applies: risk assessment, security policies, and the coordination framework elaborating the security governance and pertinent controls. Most importantly, though, within the EOSC scope there is an operational security team that concretely deals with incidents and aims to resolve them. They can leverage the information security assessments, policies, and framework, but in addition have operational capability. With that operational capability comes (i) an actionable authority with respect to the EOSC-Core, (ii) a coordinating and recommending role across the EOSC-Exchange connected services, also embodied in a Security Baseline and guidelines that are part of the EOSC AAI Implementation (for which a cross-WP working group has been established, and whose fundamentals have been laid out in the "*EOSC AAI Federation*

Participation Policy Draft" by the Working Group (WG) Architecture AAI Task Force [31]) , and (iii) a liaison role with peer infrastructures and the global security incident response community.

2.6.2.1 Risk management and transparency

Facilitating cross-service risk management needs a framework and procedures to compare and assess these risks that is consistent across the EOSC participants. Based on the WISE (Wise Information Security for E-infrastructures, wise-community.org) community standards Risk Assessment for WISE (RAW-WG) assessment template, this moves beyond any single-domain framework such as ISO 27001 and needs to be enhanced to deal with far more heterogeneous and distributed environment of EOSC participants – in which *assets* (a key concept for classifying information security risks) are not enumerable and may be less tangible than within a single organisation. In particular, the importance of research data assets, privacy, and research integrity need to be considered as *assets* in this sense. Quoting from the WISE Risk Management Template[3] : '*For example, if some data is leaked or corrupted which is stored on your system, it may not have any monetary value to you, but it probably will to someone. If personal data is accessed by a hacker, you could be fined, have a poor reputation, and people not use your system again. You could consider the asset to either be data, or reputation. Data may be leaked or corrupted due to many threats: a mis-configured system, a software vulnerability, a rogue administrator, or simply someone who releases data publicly unwittingly.*'

Taking the mentioned WISE Risk Management Template as a basis, a maturity model will be developed in which both research assets and EOSC assets (the services and community AAI proxies) are considered, and the pertinent risks for each of these are listed - itself an iterative process, reflecting the developing EOSC. Each of these risks can be self-assessed by the asset *'owner'* (resource provider, AAI service provider, or community), and graded based on the maturity of the controls addressing that specific risk. The model can then be employed to assess the risk of EOSC services and composition of such services, and through transparency – especially between service providers, communities, and users in the EOSC, allow the assessment of risk of combined and composite services – where services build on each other and thereby start sharing common risks, either aggravating or ameliorating them.

2.6.2.2 Security policy baseline and trust

Since the EOSC brings together services from many stakeholders, a mutual operational trust baseline is required to interoperate securely. Interaction between stakeholders must preserve the risk appetite of those involved, so statements on which trust is based should be open, comparably formulated, and flexible enough to address both existing and emergent usage patterns. Taking input from - amongst others - the EOSC Rules of Participation working group[4], the governance activities[5], WISE[6], and the requirements from the FIM4R community[7], baseline security policies and recommended implementation measures will be provided to the service onboarding activity, as well as to the AARC AEGIS group of e-Infrastructures, for adoption. Such policies and guidance will be provided via outputs of the project to stakeholders such as service suppliers. These will form baseline requirements for all services via the rules of participation - addressing the resource providers initially through the AAI Federation policy of which the security baseline will be an element, and operators of EOSC- Core services similarly through the "*Policy for connecting services to the EOSC-Core Infrastructure Proxy*". The AARC policy area[32] in conjunction with the Interoperable Global Trust Federation and the WISE Security for Collaboration among Infrastructures (SCI) working groups provide the policy development environment and ensure broad, and globally accepted, endorsement of these baselines which supports interoperability within and outside the EOSC scope.

There are three elements where further evolution is needed:

- Firstly, a security policy baseline to be incorporated into the EOSC AAI Federation participation policy (as prepared by the EOSC Future AAI task), including requirements for transparency and incident response participation. As the EOSC constituency grows, and becomes increasingly interdependent, successive baseline increments incorporate secure service operations guidelines (where relevant aligned with the NIS directives as they apply to research and academic organisations), appropriate operating practices for sources of authentication and authorization attributes, and identity assurance. This work is closely related to the presentation of resource providers in the EOSC portal, especially on how to present trust qualities and adherence to specific guidelines in a way that enables identification of suitable entities for (sensitive) research workflows. This baseline enables user-to-service-provider trust and provides confidence in the integrity of data sources and workflows.

- Secondly, an evolution of the trust *'mapping'* framework that WISE SCI provides by explicitly incorporating the federative aspects that exist *between* (groups of) services or infrastructures. With a much more globally distributed and heterogeneous landscape, particularly with the large Research and Education (R&E) federations, the introduction of more diverse (government) e-ID sources, and large-scale community proxies (the AARC 'community first' approach, where all trust flows form user communities), the EOSC - being a distributed system - has no single centre. This trust mapping framework enables service-provider-to-service-provider trust, and enables the composite services for which a coherent information security level can be identified
- Thirdly, an assessment of the maturity with which guidelines and baselines are implemented as an integral part of service provisioning in itself, leveraging the key research principle of *peer* review that has enabled progress in research over the years. Also, information security experience in many of the large research ICT ecosystems and e-Infrastructures has shown that peer reviewed self-assessment is an apt mechanism to demonstrate adequacy without incurring the bureaucratic and financial obstacles that traditionally come with certified audits against formal standards. Without aiming to undermine the role of ISO27k auditors, the research and academic community, and thus a large part of the EOSC participants, can benefit from a shared community background that obviates the need to spell out many of their foundational principles (the '*value system'* in which they already operate, and for which Codes of Conduct and ethical norm already exist and are well respected). This work will explicitly engage with the WISE SCI group, whose SCIv2 framework was widely endorsed by major research and e-Infrastructures, and support the evolution of that framework to establish globally consistent criteria that are (also) relevant for the EOSC, alongside an assessment model for those criteria. Establishing the mechanisms for effective peer-reviewed self-assessment of information security maturity, and the transparent exposure of the (aggregated) results, provides verifiability of trust between all EOSC participants.

In liaison with the REFEDS[8] and IGTF communities the alignment of an appropriate number of common assurance profiles and their availability will be pursued.

2.6.2.3 Incident coordination framework and an operational sharing process

Services are connected across the entire ecosystem, so while a single centrally enforced incident response for all EOSC services cannot exist, participants must still collaborate to mitigate the risk of future incidents. Similarly, information about operational vulnerabilities needs to be communicated rapidly to forestall their exploitation by malevolent actors. The coordination thereof needs a central point, as has been shown in AARC and other security incident response exercises, which is provided for here. As incidents are not limited to just one participant, their mitigation, containment, and ultimate resolution requires a collective response that spans the various areas of service offerings, all users, and service providers at a global level. The work will lever and enhance the mechanisms developed in the WISE Community [6] and REFEDS (Sirtfi)[9].

Improvements in the information sharing network require both procedures for collaborating and sharing of the so-called *'Indicators of Compromise'* (IoCs), as well as promotion of a framework in which to exchange IoCs automatically. Although the operation of such a sharing network must – by the very nature of global threats – be much wider than the EOSC, and certainly wider than the EOSC-Core, creation of an operational engagement both in the EOSC-Core services as well as in services in the EOSC-Exchange needs significant attention and thus effort.

This must be complemented by a recognised set of operational processes that can be put into action once incidents are discovered, and these processes must be periodically exercised to be effective and efficient. The EOSC needs to be engaged in (existing) pan-European networks and both participate and coordinate *'cyber-range'* exercises – considering that while for the EOSC-Core services and capabilities this is within the remit of EOSC Future, the connected services and infrastructures have their own role to play in this area, and their full participation is essential for joint success. For security incident response especially, there are no hard boundaries (since the adversaries do not respect any such boundaries either!)

2.6.2.4 Remediation of Core incidents and coordinated security response for the EOSC-Exchange

The operational security incident response capabilities will be provided by the EOSC CSIRT that needs to be mandated to coordinate security incidents involving the EOSC-Core services. These actions are run in collaboration with the services affected and will be backed by the policy set discussed earlier. To ensure successful operations, the EOSC CSIRT will use the EOSC security infrastructure (e.g. IoC sharing platform) and contact details, as well as benefit from the implemented security baselines spanning across the entire infrastructure. Relevant operational procedures and best practices will be maintained to support the function of the EOSC CSIRT and the service operators in the constituency.

Dealing with security incidents has the undeniable potential to be an unbounded challenge – and it is clear that effective remediation of incidents in the EOSC at large depends on subsidiarity: each and every service provider has a responsibility to deal with security incidents within the services they are responsible for. But at the same time, the interdependency of services requires exchange of information and a coherent and simultaneous response to incidents both across services as well as inside each individual service. For example, any local response may inadvertently signal to attackers that '*they have been found*', and thereby change the miscreant's behaviour towards other EOSC services in which they have intruded. Coordinating response is essential, and the '*EOSC Security Incident Response Team*' thus will have such coordination fully within its remit, and - following the security baseline - EOSC participants collaborate with this team. As necessary and within the (albeit limited) means available to the team, it will also help EOSC participants at large to remediate incidents. This will help prevent spreading of such incidents to other EOSC service providers and users. The EOSC CSIRT will develop and maintain trust relationships to the partners in its constituency.

The EOSC CSIRT team will position itself also in external collaborations, like established trust groups and networks of security teams and partner infrastructures.

2.7 Service Ordering and Customer Relationship Management

Service Ordering and Customer Relationship Management (SOCRM) is the process aimed at establishing and maintaining relationship with customers and it includes:

- Acting as first contact point for services requests coming from the EOSC Portal and Marketplace.
- Efficient processing of the requests for accessing services.
- Establishing and maintaining a good relationship with customers making use of EOSC services.

2.7.1 Status at the beginning of the project

Since the end of the EOSC-hub project, SOCRM has been structured around a set of five procedures:

- **Order management:** dealing with service orders from customers which includes interacting with the customer if clarifications on the request are needed and forwarding the request to the appropriate service provider.
- **Reply to contact requests:** managing and processing of the requests coming via the generic contact form of the EOSC-hub website.
- **Record and maintain information** about EOSC-hub stakeholders.
- **Provide technical support:** forwarding to the technical team requests for technical implementations and/or integrations.
- **Customer Relationship Management:** maintaining contact with customers via the comment feature in the EOSC Marketplace and collecting surveys on customers' satisfaction.

At the start of EOSC Future, the above procedures of SOCRM are at varying levels of maturity. The order management is the most mature one and it is used daily, including during the transition from EOSC-hub to EOSC Future. Customer relations management - replying to contact requests and providing technical support - is operational but still needs further refinements. Procedures covering the collection of user satisfaction and information on stakeholders are defined but not yet operational.

2.7.2 Areas for improvement

The first step that was carried out in EOSC Future was the initial review of the set of procedures from the EOSC-Hub project. After this initial analysis, it was decided to obsolete the procedure relating to recording and maintaining the EOSC stakeholder database. This was put in place when the tools used by the different procedures had not yet been finalised and thus there was a need to collect that information separately. Currently such tools are available and in fact customers (users making orders) are recorded in the EOSC Portal and the service providers are registered in the EOSC Provider Portal, thus there is no need to build a dedicated procedure and database to collect that information.

A transition phase is ongoing to set new teams (i.e. order shifters) and assign responsibilities. Other areas of improvement have been also identified and are summarised below.

A mechanism to reply to requests for information and technical support was put in place specifically for the EOSC-hub website and in line with the specific project structure; currently updated units are being defined for incoming EOSC requests via the new helpdesk structure (the details of which are still under discussion) and thus these two will be merged into one procedure which will guide on how to manage and process incoming tickets to the helpdesk.

Regarding order management, even if this is the most stable procedure within SOCRM, it is considered important to define improved mechanisms to interact with the service providers serving the orders. In particular, it would be useful to establish an improved communication channel to obtain feedback on the status of orders after they are being handed over to the target provider.

On the customer management side, the part related to maintaining contact with customers is stable and operational and no major changes are foreseen. For customer satisfaction, while the basic principles of collecting users' feedback were put in place, actual surveys were not realised during EOSC-hub and it would be an important step to have this realised in EOSC Future.

2.8 Supplier and Federation member Relationship Management

The purpose of Supplier and Federation Member Relationship Management (SFRM) is to identify suppliers of services, ensure that there is a designated contact responsible for managing the relationship and communication with the service provider and to maintain a good relationship with service providers and ensure that the supplier performance is being monitored.

2.8.1 Status at the beginning of the project

Within the EOSC SMS, SFRM was used to Identify suppliers of Hub portfolio services and project members (e-Infrastructures) who were themselves the service providers delivering these services before EOSC Future started. The process was primarily used to ensure that details are recorded and maintained for the suppliers of Hub portfolio services and that there was a designated contact on both the side of the service provider and the project, both responsible for managing the relationship between the two. The process was also designed to record any disputes between the suppliers and the project - although none were in fact recorded during the project.

2.8.2 Areas for improvement

In the area of SFRM the main work will be to establish the new contacts at the beginning of the project of all EOSC-Core services and ensure that these are maintained. From previous experience, the aspect of recording disputes is unlikely to be needed, since all suppliers of EOSC-Core services are partners within the project and the Collaboration Agreement largely fulfils the purpose of establishing and maintaining a good relationship. However, the existing procedure for recording disputes will likely be retained.

3 Service Operation and Control

3.1 Incident and Service Request Management

The Incident and Service Request Management (ISRM) process is one of the major operational processes which ensures the stable operation of the infrastructure and defines a set of procedures and policies for the restoration of normal and agreed service operation within the time after the occurrence of an incident that is agreed within SLM. It also provides a way for users to communicate with service providers allowing them to ask for help, report a problem, make a feature request etc. The ISRM process is interfaced with other operational processes like Change Management, Configuration Management, Problem Management which is required for the successful operations of the infrastructure.

3.1.1 Status at the beginning of the project

The ISRM process was established in the first year of the EOSC-hub project together with main incident and request management procedures, policies, and a multi-level structure of support units. Based on the requirements of the ISRM process, the helpdesk service was deployed in the EOSC-hub project and integrated with EGI and EUDAT helpdesks. The ISRM was successfully executed and constantly enhanced during the EOSC-hub project period. At the beginning of the EOSC Future project the ISRM represents a mature process running in production with focus on the EOSC-Core services and their operations.

3.1.2 Areas for improvement

The change from EOSC-hub to EOSC Future project requires thorough review of the current ISRM process, its procedures, and policies. Many requirements of EOSC communities and EOSC users which have been collected previously have to be accurately assessed and implemented in process and related services and tools.

Considering the growth of the EOSC infrastructure the coverage of the ISRM process should be extended to the EOSC constituents beyond the EOSC-Core. It is important to mention that many of the services outside of the EOSC-Core are operated by service providers based on their own processes and procedures, thus the enhancement of the ISRM process should focus on the interfaces to the external processes rather than on inclusion of the external well-defined processes in the EOSC ISRM.

While the focus in the EOSC-hub project was given to establishment and full specification of the ISRM process, it is considered that more effort is required for the definition of the interfaces to other EOSC SMS processes mentioned in introduction of the Section 3.1. According to the FitSM standard the main SMS processes to which the interfaces should be in place are:

- **Change Management**
  - The tickets submitted to the Helpdesk and classified as Requests for Changes (RfC) should be seamlessly propagated to and registered in the Change Management for further evaluation and eventual approval.
- **Problem Management**
  - Although the procedure ‘How to report an incident and service degradation’ has been developed, it was rarely in use by service providers. Due to missing integration between the monitoring and helpdesk systems the service providers had to manually report on service degradations and incidents. The procedure needs to be reviewed and the usage of this procedure should be improved. Although not all the incidents, e.g. security incidents, can be detected by the monitoring system and some of the incidents still have to be reported by creating a ticket manually, a significant improvement of the reporting of service degradation is expected by integration of the monitoring and helpdesk systems. In this way, all incidents and service degradations detected by the monitoring system will be registered automatically for further assessment and review.
  - Service incidents and service requests should be accessible by the Problem Management process to identify problems, perform trend analysis. The identified problems and workarounds should be recorded in the Known Error Database (KEDB).
- **Configuration Management:**

  - All service incidents and requests submitted by users or service providers should be assigned to the corresponding EOSC-Core service in the Configuration Management Database to facilitate other processes like Problem Management, Change Management, Service Level Management which could require this information for analysis and reporting.
- **Service order and customer relationship management:**
  - An improved integration with SOCRM is needed to provide better technical support related to orders and the order management system itself.

3.2 Problem Management

3.2.1 Status at the beginning of the project

The main objective of the Problem Management process is the prevention of the recurrence of the incidents by investigation of the root causes of the reported incidents. The output of the Problem Management is the registry of identified problems, workarounds and temporary fixes till the problem is permanently solved.

During the EOSC-hub project the process has been established together with main procedures. The focus of the process was only operational incidents in the EOSC-Core infrastructure. A Known Error Database has been created. The rate of long recurring problems was low in the infrastructure, and most of the operational incidents were quickly resolved within a few days after reporting, with the number of the records in KEDB based on the results of problem analysis being low.

3.2.2 Areas for improvement

As it has been previously noted, the PM process has been rarely used and the Known Error Database contains just a few records related to EOSC-Core services. The reason for that is the low rate of submitted service incidents by service providers, quick fixes have been performed after a problem has been detected.

To improve the process, it is proposed to review Problem Management procedures in the EOSC Future project, define the types and scope of the problems to be handled by the process, define a better interface to the ISRM process and implement it in the Helpdesk service. A better interface to the ISRM process would also allow efficient trend analysis based on statistics of incidents and service requests. The information about major workarounds could be provided to the ISRM process for publishing in the FAQ section in Helpdesk portal available for users.

3.3 Change Management

The goal of the EOSC Change Management process (CHM) is to ensure that changes to services are planned, approved, implemented, and reviewed in a controlled manner, such that the negative impact of changes to services and ultimately to customers can be avoided. The CHM plays an important role in the federated environment, where changes on Configuration Items could affect other federation members, which might not be foreseeable by the person requesting the change.

The actual running process provides procedures for three types of changes: **Emergency Changes**, **Standard Changes** and **Non-standard Changes:**

- **Emergency Changes** are changes that need immediate action, like, for example, software updates to fix security threats.
- **Standard Changes** are evaluated once for their risk and impact on the Service Management System (SMS), and, if approved, added to the List of Standard Changes, such that they are pre-approved on subsequent occasions.
- The remaining changes are **Non-standard Changes**, which are assessed by a Change Management procedure to be of low or high risk.

High-risk changes can only be approved through the Change Advisory Board (CAB). The CAB is a board that consists of senior project members and, if necessary, external experts able to make decisions on requested changes. It is called by the Change Manager to review and decide on any problem related to the CHM process, including but not limited to the review process after Emergency Changes and the decision to mark a change as a Standard Change.

3.3.1 Status at the beginning of the project

The CHM process that was developed within EOSC-hub is a mature process and has been running over the last two years prior to the start of EOSC Future. All procedures and policies together with auxiliary tools have been finalized and were subject to three audits during the EOSC-hub project achieving positive feedback from the reviewers.

The Change Management is not directly accessible from the outside but is sheltered from external requests by other processes. However, Requests for Changes (RfCs) can in principle be raised by anybody inside the EOSC SMS.

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

3.3.2 Areas for improvement

The CHM process, including policy and procedures, has been defined and built taking into consideration the EOSC-hub environment. This means that the scope and procedures need to be reviewed and adapted to the new EOSC ecosystem. Also, the auxiliary tools used by CHM, Jira and Confluence, need to be re-evaluated and adapted to the new services. Also, a new set of examples and tutorials on how to treat already approved standard changes need to be made together on how to define the best way of communication and to improve the interaction of all other EOSC processes.

3.4 Configuration Management

The Configuration Management of the EOSC (CONFM) provides and maintains a logical model of all EOSC-Core services and their relationships and dependencies. It forms the basis and central point of information provision for all processes of the EOSC that need to obtain, store, or update information from the EOSC-Core services. This includes interaction with the Change Management (CHM), the Problem Management (PM), Incident and Service Request Management (ISRM), as well as the Service Availability and Capacity Management (SACM). Configuration Management also facilitates the decision-making process, either at the SPM level or at any other governance level concerning inclusion or exclusion of one or another service in the EOSC-Core. The most important feature of the CONFM is the Configuration Management Database (CMDB) which stores the relevant information necessary to run the EOSC-Core Services.

3.4.1 Status at the beginning of the project

The scope of the configuration management process has already been defined together with the identification of the Configuration Management Database (CMDB). Based on the CONFM scope, the CI types and attributes needed to run the EOSC services were defined together with a proposed topology compliant for all EOSC services: both EOSC-Core services and EOSC-Enhanced. The requirements are described in the EOSC-hub Configuration Management Plan[10] which was open for consultation under the EOSC project. Based on this model an initial CMDB implementation based on a confluence space was created.

3.4.2 Areas for improvement

The current implementation of the CMDB for EOSC it is still in an early stage and currently, it is based on a confluence space that does not comply with some of the CMDB requirements like for example automatic check of the DB or automatic detection of service attribute changes. Under EOSC Future a new CMDB implementation is being prepared by WP4 with contribution from WP7. The topology adopted for the services will follow the Configuration Management Plan [10] elaborated by the EOSC Future project.

3.5 Release and Deployment Management

The Release and Deployment Management (RDM) process oversees the implementation of approved changes into production. Therefore, all changes to the EOSC-Core services approved by the EOSC-hub Change Management are required to follow the Release policy. The RDM operates in conjunction with the CHM.

3.5.1 Status at the beginning of the project

The Release and Deployment Management (RDM) process is fully operational and integrated in the CHM process. The RDM consists of a series of procedures, policies and guidelines that oversee and help service providers in their new releases of the services into production.

3.5.2 Areas for improvement

The defined policy and procedures in the RDM clearly identify different types of release such as major, minor, and emergency within a predefined schedule. However, it needs improvement regarding the creation and latter adoption by the service providers of guidelines and best practices for software releases. The improvement and adoption of these guidelines and best practices require a wider scope in the project and to tackle this a cross package working group dedicated to the Software Quality Assurance was proposed and approved by the Technical Collaboration Board (TCB).

3.6 Continual Service Improvement

At the beginning of the project, it was decided that the various software quality activities should be combined to provide guidance for all the technical Work Packages, rather than being introspective. Therefore, an initiative was launched, relating to Continual Service Improvement (CSI) for the software developed within EOSC, particularly for the EOSC-Core. It was felt that this is a specific activity of the CSI process within the SMS. However, due to the specialized nature of this activity, it is covered within its own dedicated section within this document, alongside CSI for the SMS.

3.6.1 CSI for Services

Continual Service Improvement (CSI) for Services is an extension of CSI for SMS and is an initiative launched towards the beginning of the EOSC Future project to support the quality assurance and service development activities in a coordinated manner. Consolidating existing know-how within the project to provide documentation that supports Software Quality Assurance (SQA)[11] will facilitate the development of consistently high-quality services and releases for the EOSC-Core. It is also hoped that this work may be useful for software developers external to the project who are interested in joining the EOSC ecosystem (or who have already onboarded to EOSC).

3.6.1.1 Status at the beginning of the project

Software Quality Assurance (SQA) today plays a critical role in *'defining and assessing the adequacy of the processes to produce software products of suitable quality for their intended purposes'* [12] and this fact shall also be true for all the software-enabled EOSC services. Hence, this implies having well-established software engineering methods, procedures, and tools. The procedures should be aligned with existing standards and well-established guidelines and should be applied throughout the software development life cycle.

The Common Software Quality Assurance Baseline Criteria[13] document, developed by the INDIGO-DataCloud project and later enhanced by DEEP-Hybrid-DataCloud and EOSC-Synergy projects, establishes a minimum set of quality requirements for any software development project, but mainly oriented to research. This document served as an input for the current EOSC SQA technical specification[14] , which includes a set of interoperability guidelines that EOSC-Core services should comply with. These technical specifications also include a list of software products, part of the EOSC-hub Common services, and thus delivered through the EOSC portal, that was compliant with those guidelines. It also contains references to a library[13] that provides the practical means (incl. automated testing) for software projects to adopt the common SQA practices identified within the document. The library is currently being redesigned under the framework of the EOSC-Synergy project[33] to improve its usability while coping with the requirements of the SQA as a Service (SQAaaS) platform, which is meant to streamline the adoption of SQA practices in research software. The EOSC association already provides guidance and best practices for the release of software-based servicestogether with a detailed configuration management plan[10] on how to integrate services into the EOSC association.

The CESSDA Software Maturity Levels[19] specify eleven criteria that should be addressed and provide a scoring guide and minimum and expected scores for each criterion. The minimum/expected scores can be customised to provide domain-specific profiles if required. The CESSDA Software Development Guidelines[24] provide a comprehensive *'best practice'* narrative for developers to follow. The EURISE Network provides a Software Quality checklist[20] as part of a wider set of guidelines for software developers. Collectively, this set of specifications, procedures and software libraries refers to and builds on many standards and initiatives from beyond the EOSC landscape, so there is no intention to perform another review of that landscape here. However, there are some complementary initiatives that have benefited from EU funding and/or support and should be taken into consideration They have been chosen because, although there is a good deal of overlap between their scope and that of the EOSC SQA activities mentioned above, there is the possibility to combine aspects of them to good effect.

It should be noted that EOSC Enhance uses the following tools and techniques (based on Github Actions[25]) for SQA of the components that it is producing:

Code branch/Pull Request deployment

- feature acceptance tests
- manual exploratory testing
- end-to-end blackbox tests (Cypress)
- integration / UI testing (Capybara)
- unit tests (RSpec)

Main branch deployment

- manual exploratory testing
- end-to-end blackbox tests
- integration / UI testing
- unit tests
- application-level errors monitoring (Sentry)

Beta deployment

- manual testing for both exploratory testing and full test suite (TestQuality)
- release acceptance testing
- integration testing, including external interfaces integration tests
- application-level errors monitoring

Production deployment

- manual testing, mostly sanity checks
- integration testing
- application-level errors monitoring

Where possible, their effectiveness will be evaluated to see if some or all of them should be carried forward into this project.

3.6.1.2 Areas for improvement

A comparison of the criteria covered by the various guidelines referred to above shows the following:

- The areas of Licensing/IP, Documentation, Code accessibility, Security, Citation/metadata are well represented.

- There is a *'long tail'* of items that are only mentioned in one or two of the guidelines. They require further investigation to determine if they have been generally overlooked or are deliberately excluded for being less relevant than the others.

Providing an automated testing facility for criteria that are not currently covered is significant improvement, as manual regression testing is not a realistic option across a project the size of EOSC Future. One example would be to use the guidance given in the Documentation section of[16] (as to what each of the technical documentation types should contain) then parse documents to see if they are present. This would not necessarily be a simple pass/fail test, as it could be appropriate to use a minimum/recommended score that depends on the file type. This largely depends on adopting a docs-as-code approach, as recommended by some of the quoted guidelines, so that easily analysable plain text files are available in a source code repository.

It is worth noting that the five recommendations for making software FAIR[6] are a subset of the criteria covered by the various guidelines under consideration. It is therefore within the scope of the SQA activity to ensure that the software components of the EOSC-Core Services are FAIR[17].

The Technical Coordination Board has agreed that a cross-Work Package working group on Software Quality Assurance should be established. Consisting of members of WP3, WP4, WP5, WP7 and WP10, it will carry out the following tasks:

SQA 1: Survey covering the initial status of SQA (M4)
This will be directed at EOSC-Core service developers and contributors to the EOSC-Exchange Portfolio. It is intended to discover to what extent those teams developing/enhancing software for EOSC understand the concept of Software Quality Assurance (SQA).

SQA 2: Follow up survey regarding SQA (M8)
This will be directed at the EOSC-Core service developers and contributors to the EOSC-Exchange Portfolio. It is intended to discover details of the processes and tools used by those teams developing/enhancing software for EOSC.

SQA 3: Publishing of SQA guidelines on EOSC Future **wiki (M9)**
Based on an analysis of the responses to the two surveys, and further examination of the '*long tail*' criteria, some initial SQA guidelines will be produced and made available to the EOSC Future software development community.

SQA 4: Establishment of a methodology of assessing SQA compliance (M12)
Based partly on an analysis of the responses to the survey questions about minimum standards for SQA, a methodology will be devised to assess whether the mandatory/advisory (yet to be determined) standards are being adhered to. Feedback will be sought from the EOSC Future software development community.

SQA 5: SQA compliance methodology implemented (M15)
Following consultation with the EOSC Future software development community, the methodology will be implemented in pilot form.

SQA 6: SQA compliance methodology run across all EOSC-Core services (M30)
The pilot will be gradually expanded until it covers all EOSC-Core services. The work is being done under the auspices of a cross Work Package Group (XWP) endorsed by the Technical Control Board (TCB), so adoption is expected to be widespread within the technical Work Packages.

SQA 7: Alignment with outputs of EOSC Task Force on Infrastructures for Quality Research Software (Ongoing)
Liaison with the Task Force will take place on a regular basis, to ensure where possible that outputs are aligned.

3.6.2 CSI for the SMS

The purpose of Continual Service Improvement (CSI) of the Service Management System (SMS) is to identify, prioritize, plan, implement and review improvements to services and the service management system itself.

3.6.2.1 Status at the beginning of the project

At the end of the EOSC-Hub project, CSI for the SMS was done by supporting the creation of CSI Jira tickets associated with all the SMS processes as well as tracking the workflow of the approval and implementation of the improvement suggestions. CSI accepted over 100 suggestions for improvement from a number of sources:

- during periodic SMS process reviews
- feedback from auditors during the SMS audit program
- anyone with a proposal for implementation of the SMS and its processes

CSI was set up to ensure that this process within the EOSC SMS effectively supported the PDCA (Plan - Do - Check - Act) Deming cycle[26] to ensure a continuously improving SMS.

3.6.2.2 Areas for improvement

It is not considered that anything fundamental needs to change with the approach of CSI at the SMS level, other than making all users of the SMS within EOSC Future aware of the process, what it is for and how it functions.

4 Conclusion

This deliverable aims at providing a comprehensive overview of the Service Management System (SMS) supporting the portfolio of EOSC services and the development, maintenance, and service delivery of the EOSC Portal and EOSC-Core technical services. This covers the status of the processes, procedures, and policies as of this point of the project, along with plans for how to further develop this work over the course of the project to ensure that it meets the needs of the project and stakeholders including the end users of EOSC services. This deliverable contains a detailed section on Security as this may be viewed as an EOSC service, albeit a largely non-technical one, and as such it is a service being developed exclusively within the SMS.

5 References

[1] EOSC Architecture Working Group view on the Minimum Viable EOSC https://op.europa.eu/en/publication-detail/-/publication/91fc0324-6b50-11eb-aeb5-01aa75ed71a1/language-en

[2] *Trust Coordination for Research Collaboration in the EOSC era* https://doi.org/10.5281/zenodo.3674676

[3] WISE Risk Management Template https://wise-community.org/risk-assessment-template/

[4] EOSC Rules of Participation working group https://www.eoscsecretariat.eu/working-groups/rules-participation-working-group

[5] EOSC Governance Activities https://www.eoscsecretariat.eu/eosc-governance/eosc-executive-board-outputs

[6] WISE, https://wise-community.org/sci/

[7] FIM4R, Federated Identity Management for research, https://fim4r.org/documents/

[8] REFEDS, Research and Education Identity Federations, https://refeds.org/

[9] REFEDS Sirfti, https://refeds.org/sirtfi

[10] Pavel Weber, Isabella Bierenbaum, Joao Pina. (2021, March 11). EOSC-hub Configuration Management Plan (Version 1). Zenodo. http://doi.org/10.5281/zenodo.4040865

[11] Software Quality Assurance; Wikipedia; https://en.wikipedia.org/wiki/Software_quality_assurance

[12] Guide to the Software Engineering Body of Knowledge, SWEBOK http://swebokwiki.org/Chapter_10:_Software_Quality

[13] A library to implement Software Quality Assurance (SQA) checks in Jenkins environments; Orviz, Pablo; Bernardo, Samuel; Rodgon, David; Castroa, Marta; EOSC-Synergy project; https://github.com/indigo-dc/jenkins-pipeline-library

[14] EOSC Technical Specification Software Quality Assurance; version 1.0; INDIGO-DataCloud, DEEP-Hybrid-DataCloud and EOSC-Synergy projects;https://wiki.eosc-hub.eu/display/EOSCDOC/Software+Quality+Assurance?preview=/63440177/64916281/EOSC%20Technical%20Specification-SQA%20.pdf

[15] jenkins-pipeline-library: automate the SQA task; EOSC-Synergy project; https://indigo-dc.github.io/jenkins-pipeline-library/2.0.0/index.html

[16] A set of Common Software Quality Assurance Baseline Criteria for Research Projects; Indigo, Deep and EOSC Synergy; https://indigo-dc.github.io/sqa-baseline/

[17] FAIR Software; Netherlands eScience Center and DANS; https://fair-software.nl/

[18] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18

[19] CESSDA Software Maturity Levels; CESSDA ERIC; https://docs.tech.cessda.eu/forms/sml.html

[20] Software Quality Checklist; EURISE Network; https://technical-reference.readthedocs.io/en/latest/quality/software-checklist.html

[21] RDM Guidelines and best practices for software releases; EGI; https://confluence.egi.eu/display/EOSC/RDM+Guidelines+and+best+practices+for+software+releases NOT ACCESSIBLE TO THE PUBLIC

[22] EOSC Common Services https://www.eosc-hub.eu/topic/common-services

[23] EOSC-Synergy Software Quality as a Service (SQaaS) https://sqaaas.eosc-synergy.eu

[24] CESSDA Software Development Guidelines, https://docs.tech.cessda.eu/software/ta-sw-dev-guide.html#documentation-throughout-the-development-life-cycle

[25] Github Actions., https://docs.github.com/en/actions

[26] PDCA Deming cycle https://en.wikipedia.org/wiki/PDCA

[27] FitSM Standards Family, https://www.fitsm.eu/

[28] Hub Participation Agreement https://wiki.eoscfuture.eu/display/EOSCSMS/SLM+Agreements+and+templates NOT ACCESSIBLE TO THE PUBLIC

[29] Service Reports Catalogue https://wiki.eoscfuture.eu/display/EOSCSMS/Process+reports+catalogue NOT ACCESSIBLE TO THE PUBLIC

[30] Capacity Plan template https://wiki.eoscfuture.eu/display/EOSCSMS/Capacity+Plan+template NOT ACCESSIBLE TO THE PUBLIC

[31] EOSC Authentication and Authorization Infrastructure (AAI) Report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF), ISBN 978-92-76-28113-9

[32] AARC Policy Development Kit https://aarc-community.org/policies/policy-development-kit/

[33] EOSC Synergy project https://www.eosc-synergy.eu/