D7.2 Status of the SMS Processes

Lead partner:	EGI Foundation
Version:	1
Status:	Final
Dissemination Level:	Public
Keywords:	EOSC, SMS, Processes, ECP
Document Link:	https://documents.egi.eu/document/3807

Deliverable Abstract
EGI-ACE is one of the service provider projects of EOSC. EGI-ACE delivers over 30 services that form the 'EOSC Compute Platform' (ECP) and thematic services that rely on the ECP to provide scalable data analytics environments for domain researchers. Majority of the EGI-ACE services are managed through the ISO 20k compliant service management system (SMS) of the EGI Foundation. This deliverable introduces this SMS and provides guidance to those new providers who want to join the EOSC Compute Platform and therefore need to comply with certain SMS processes. The document also provides an overview of the interfaces between the EGI-ACE SMS and EOSC SMS.

COPYRIGHT NOTICE

EGI-ACE receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101017567.

DELIVERY SLIP

	Name	Partner/Activity
From:	Alessandro Paolini	EGI Foundation/WP7
Moderated by:	Sjomara Specht	
Reviewed by:	Sebastian Luna Valero Malgorzata Krakowian Gergely Sipos	EGI Foundation EGI Foundation EGI Foundation
Approved by:	SDS	

DOCUMENT LOG

Issue	Date	Comment	Author
v.0.1	11/03/2022	Version ready for the reviewers.	A. Paolini, B. Grenier, E. Testa, G. Larocca
v.0.2	13/03/2022	Addressed comments from reviewers	A. Paolini, M. Krakowian, S. Luna Valero, G. Sipos
v.1	13/03/2022	Final	A. Paolini

TERMINOLOGY

https://confluence.egi.eu/display/EGIG

Terminology/Acronym	Definition
CAPM	Capacity Management
CHM	Change Management
CONFM	Configuration Management
CSI	Continual Service Improvement
CRM	Customer Relationship Management
ISRM	Incident and Service Request Management
ISM	Information Security Management
PM	Problem Management
RDM	Release and Deployment Management
SACM	Service Availability and Continuity Management
SLM	Service Level Management
SPM	Service Portfolio Management

SRM	Service Reporting Management
SUPPM	Suppliers Relationship Management

Contents

Executive summary

The EGI Foundation has established a Service Management System (SMS) to deliver its IT-Services holding an ISO/IEC 20000 certification-1:2018. This is an international standard that outlines the requirements for design, transition, delivery and improvement of IT services that fulfil service requirements and provide value for both the customer and the service provider. The ISO/IEC 20000-1:2018 standard demonstrates excellence and proves best practice in IT service management. The EGI Foundation SMS is also structured and organised into processes and procedures according to the FitSM IT Management standard, a free, pragmatic, lightweight, and achievable standard aimed at facilitating service management in IT service provision, including federated scenarios.

The EGI-ACE service portfolio is composed of services that are governed by the EGI Foundation, and therefore are managed by the EGI Foundation SMS, and services that are provided by the broader EGI community and therefore currently fall outside the EGI Foundation SMS. This deliver has therefore dual perspectives:

- It introduces the EGI Foundation SMS, from the perspective of service providers, providing guidance to those who wish to join the EGI Foundation services (https://www.egi.eu/services) of EGI-ACE as new resource providers (e.g. as a new federated cloud Resource Centre).
- It provides an overview of service management status of the non-EGI Foundation services of EGI-ACE, providing focus for existing and new EGI-ACE providers on critical elements of service delivery. (Such as availability/reliability monitoring, tracking of changes, handling user requests)

The EGI Foundation SMS is a similar system that EOSC is introducing for the EOSC Core services in the EOSC Future project, and to some extent enforcing on the providers who onboard services to the EOSC Exchange. EGI-ACE meets the requirements demanded by EOSC Future in this respect and integrates with the Service Portfolio Management (SPM), Customer relationship management (CRM), Incident and service request management (ISRM) processes of EOSC.

The main objective of the service management in EGI-ACE for the remaining 15 months is to expand the scope of the existing EGI Foundation SMS to the whole EGI-ACE portfolio, reaching an SMS that can act as an umbrella above both the EGI Foundation services and services contributed by the EGI community. This document takes initial steps in this direction, the full report is planned in D7.5 in May 2023.

1. Introduction

EGI-ACE is a 30-month project (Jan 2021 - June 2023) with a mission to empower researchers from all disciplines to collaborate in data- and compute-intensive research through free-at-point-of-use services that are delivered through EOSC.

By building on providers from the EGI Community, EGI-ACE delivers

(1) the EOSC Compute Platform (ECP), a federated system of compute and storage infrastructure extended with platform services to support diverse types of data processing and data analytics cases. The ECP currently includes High Throughput Compute (HTC) and Cloud Compute facilities and will broaden its scope with High Performance Compute services later in 2022. The platform layer of the ECP provides assistance for single sign-on, for the transfer and federation of distributed data, for interactive computing, for the management of large number of jobs, for the orchestration of compute clusters, for AI and machine learning tasks. Approximately half of the services of the EOSC Compute Platform are 'EGI Foundation' services (i.e. governed and managed by the EGI Foundation), the rest are contributed by the EGI Community.

(2) A growing portfolio of (currently 18) thematic services (data spaces and data processing platforms) that integrate data and applications from different scientific disciplines into the ECP for the scalable analysis and exploitation of scientific datasets. Moreover, 10 additional thematic services, from outside the consortium, are also available in the EOSC Portal as result of support received from the ECP. All the thematic services are provided by the EGI Community outside the EGI Foundation service management scope.

In 2016 the EGI Foundation established a Management System for its IT-Services fulfilling the requirements from the ISO/IEC 20000-1:2018 standard (referred to as EGI Foundation SMS in the rest of the document). ISO/IEC 20000-1:2018 is an international standard that outlines the requirements for design, transition, delivery and improvement of IT services that fulfil service requirements and provide value for both the customer and the service provider. The ISO/IEC 20000-1:2018 standard demonstrates excellence and proves best practice in IT service management. EGI Foundation obtained the certification in 2016 and since then has remained certified by undergoing regular audit processes.

The EGI Foundation SMS is structured and organised into processes and procedures according to the FitSM IT Management standard[1]. FitSM is a free, pragmatic, lightweight and achievable standard aimed at facilitating service management in IT service provision, including federated scenarios. For each of the processes (there are 14 of them, see Section 4 for more details) FitSM defines a small number of implementation requirements[2] and provides guidelines[3] on the activities to set up and implement IT Service Management

[1] FitSM IT Service Management standard: https://www.fitsm.eu/
[2] FitSM-1 document - Requirements: https://www.fitsm.eu/downloads
[3] FitSM-2 document - Objectives and Activities: https://www.fitsm.eu/downloads

(ITSM) using these processes. The FitSM-3 document[4] describes the proposed roles to be assigned to execute the ITSM processes as part of a service management system. Both FitSM and ISO/IEC 20000-1:2018 specify requirements for a SMS, are compatible, and complement each other.

Section 2 contains an overview of the relation between the EGI-ACE services and the EGI Foundation SMS. Because the EGI-ACE service portfolio is broader than the EGI Foundation service portfolio, not all the EGI-ACE services are managed through the EGI Foundation SMS. One of the objectives for the SMS work in EGI-ACE is to bring the whole EGI-ACE service portfolio under a single umbrella, expanding the EGI Foundation SMS to an 'EGI SMS' that offers management processes for both the EGI Foundation services and services provided by the EGI Community.

In Section 3 we provide a list of activities that an EOSC provider should undergo in order to join the EOSC Compute Platform. There are two cases here:

(1) Providers who want to join for one of the EGI Foundation services. This route relies on procedures defined in the SMS and this deliverable makes it clear how the whole SMS supports such integration process
(2) Providers who want to contribute with a new service. This route is custom and requires provider-side implementation of those topics that are described in Section 3.

In Section 4 we provide a full listing of the EGI Foundation SMS processes along with the list of requirements that come from the SMS standards. Since FitSM-1 follows a more lightweight approach compared to ISO/IEC 20000-1:2018, the requirements of FitSM-1 can be regarded as a subset of the requirements covered by ISO/IEC 20000-1:2018. That is why, besides the FitSM-1 requirements, we listed a series of additional requirements from ISO/IEC 20000-1:2018 that must be fulfilled if an organisation/IT Provider strives for a certification of their SMS against ISO/IEC 20000-1:2018 but wants to use FitSM-1 as their core ITSM framework / standard.

In Section 5 we provide an overview of the EOSC SMS, and its demand on providers of the EOSC Exchange (one of which is EGI-ACE). The section details how the EGI-ACE SMS meets all the requirements that EOSC Future enforces on EOSC Exchange providers.

[4] FitSM-3 document - Role model: https://www.fitsm.eu/downloads

2. EGI-ACE services and EGI SMS

The EGI-ACE project integrates services from the EGI Foundation, as well as from the broader EGI community. The services of the EGI Foundation are governed by the EGI Council[5] and are grouped into two service portfolios:

- External services[6] (or EGI Services in short) target scientists, multinational projects and research infrastructures and are provided by EGI's federated cloud providers and data centres. The services can be requested by everyone involved in academic research and businesses via the EGI Marketplace[7] and recently via the EOSC Marketplace[8]. The External services are part of the 'Federated resource providers', the 'Compute and data federation' and the 'Platforms' layers of the EOSC Compute Platform (see Figure 1). EGI external services are sustained from a mix of national funds and EGI Council membership fees.
- Internal services[9] are provided for the benefit of the EGI Council members and affiliated organisations. The internal services complement the EGI Services for academia and business with tools designed to facilitate coordination and improve how the EGI Federation works together. The EGI internal services form the 'Service Management tools' pillar of the EOSC Compute Platform (Fig. 1). The EGI Internal Services are sustained as part of the EGI Federation, with a co-funding mechanism supported jointly by the EGI Council members, and by the service suppliers themselves. As such these services are sustained completely independently of EOSC and have been brought to EGI-ACE as self-contribution.

[5] EGI Council members: https://www.egi.eu/about/egi-council/
[6] EGI External services: https://www.egi.eu/services/
[7] https://marketplace.egi.eu/
[8] https://marketplace.eosc-portal.eu/
[9] EGI Internal services: https://www.egi.eu/internal-services/

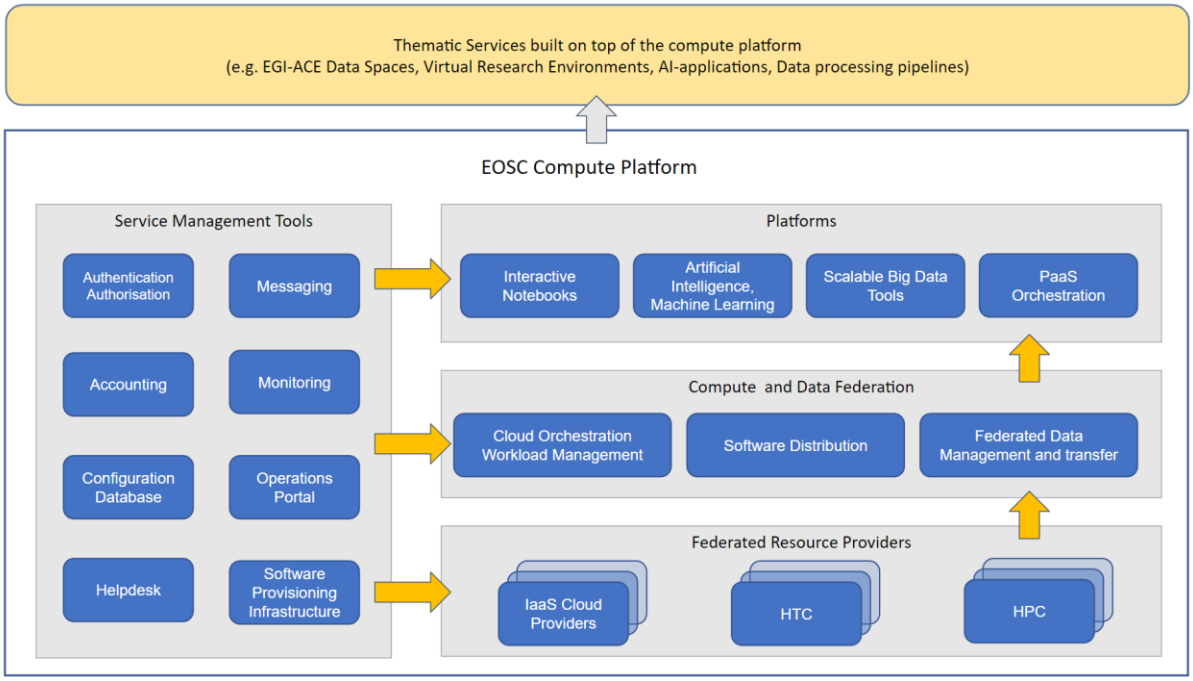

Figure 1. EOSC Compute Platform functional block diagram

The EGI-ACE services relate to the EGI SMS in one of these three ways:

1. Some of the EGI-ACE EOSC Compute Platform services are already governed by the EGI Council (i.e. they are in the EGI External or Internal portfolios) therefore are covered by the EGI SMS:
    a. Within the Federated Resource Providers layer: Cloud Compute, HTC Compute, Cloud Container Compute, Online Storage.
    b. Within the Compute and Data Federation layer: Check-in, DataHub, Data Transfer (FTS)
    c. Within the Platforms layer: Notebooks, Workload Manager
2. Some of the EGI-ACE EOSC Compute Platform services are not (yet) included in the EGI Service portfolios, therefore their management is not yet covered by the EGI Foundation SMS:
    a. Within the Federated Resource Providers layer: DynamicDNS, HPC Compute (new service still in development).
    b. Within the Compute and Data Federation layer: AppDB, Infrastructure Manager, OpenRDM, CVMFS, RUCIO.
    c. Within the Platforms layer: EC3, DODAS, Indigo PaaS Orchestrator, DEEP training solution, Binder.
3. EGI-ACE thematic services (Data space services) are not covered by the EGI SMS at all.

The project intends to raise the maturity of the services in group 2 and 3 by bringing them under the EGI SMS. The existing level of service management of these services is an important consideration for this work. As the first step the project performed a preparatory activity, the maturity assessment of the services in Group 2. The assessment focused on

Group 2, because this a more stable group than the very dynamically expanding Group 3, and because the providers in this layer are directly linked to the EGI Governance through the EGI Council. From the operational perspective the important aspects of an SMS are to ensure that:

- the services are monitored (to ensure they work as expected);
- the support is properly defined and provided (to handle incidents and service requests);
- they are registered in the Configuration Database (so changes can be tracked, and status information can be obtained for monitoring);
- Capacity plans and Availability and Continuity plans are available for them.

The updated status of this assessment is summarised in Table 1.

Table 1: Maturity status of the EGI-ACE Compute Platform services that are outside of the EGI Foundation SMS.

EGI-ACE service	Monitored?	Has a Helpdesk support unit?	Has an entry in the Configuration Database?	Has a capacity plan?	Has an availability and continuity plan?
EOSC Compute Platform: Compute and data federation services					
DynamicDNS	YES	YES	YES	NO	YES
AppDB	YES	YES	YES	NO	YES
Rucio	YES	YES	YES	NO	YES
OpenRDM	YES	YES	YES	NO	NO
CVMFS	YES	YES	YES	YES	YES
EOSC Compute Platform: Platform services					
EC3	YES	YES	YES	NO	YES
Infrastructure Manager	YES	YES	YES	NO	YES

DODAS	**NO**	**YES**	**YES**	**NO**	**NO**
Binder	**YES**	**YES**	**YES**	**YES**	**YES**
Indigo PaaS Orchestrator	**NO**	**NO**	**YES**	**NO**	**NO**
DEEP training solution	**NO**	**NO**	**YES**	**NO**	**NO**

Since the beginning of the project, the work to bring these services under the EGI Foundation SMS has been started and for most of them the aspect still missing is the creation of a capacity plan. There are two directions that can be taken with these services:

- bring them into the existing EGI governance, implying a full integration with our SMS;
- choose a 'lightweight' SMS integration approach, with e.g. requiring maturity in the areas covered in Table 1, as well as maturity in some user-facing activities especially Customer Relationship Management and Service Level Management. These requirements could be formulated in a new, 'lightweight SMS' that would apply to the services that EGI includes in its portfolio but that will not be sustained like the Internal Services.

Deciding on the direction to make with these services is work in 2022 for Task 2.2, the affected service providers, and the EGI Services and Solutions Board (SSB)[10].

[10] https://confluence.egi.eu/pages/viewpage.action?pageId=132186565

3. Joining the EOSC Compute platform

We describe in this section the set of actions a service provider should follow to join the EOSC Compute platform and to ensure the high-quality delivery of service according to the EGI policies. In particular, we consider here 6 cases:

1. Joining as a federated resource provider. A provider (that we call Resource Centre) delivering one of the existing EGI Foundation services within the Federated Resource Providers layer: Cloud Compute, HTC Compute, Cloud Container Compute or Online Storage.
2. Joining as a software provider, also called Technology Providers[11], which are the maintainers of the middleware deployed on the 'federated resource providers' (previous point), enabling compute and storage services.
3. Joining as a new provider of the EGI Foundation services that are already included in the Compute and Data Federation or the Platform services blocks (e.g. Workload Manager, Notebooks, DataHub, …).
4. Joining as a new provider of an existing, non-EGI Foundation service in the Compute and Data Federation or the Platform services blocks (e.g. IM, EC3, DODAS, …).
5. Joining as Core/Central service provider within the Service Management Tool block: providers that support all the other services of the EOSC Compute Platform.
6. Contributing a new (i.e. not yet present) service to the EOSC Compute platform (to the Federated Resource Providers, Compute and Data Federation, or the Platform services blocks).

Integrating a new Thematic Service with the ECP is outside the scope of this listing and one can do that by receiving support from EGI-ACE, most appropriately through the 'EGI-ACE Call for Use Cases'[12].

3.1 Federated resource providers - Resource Centres

A Resource Centre (RC) is the smallest resource administration domain in the EGI Federation. It can be either localised or geographically distributed and provides a minimum set of local or remote IT Services compliant with well-defined IT Capabilities (HTC, Cloud, Storage, etc.) necessary to make resources accessible to Users. EGI is a Resource Infrastructure federating RCs to constitute a homogeneous operational domain.

3.1.1 Registration and certification

In order to join the EOSC Compute platform, a RC needs to present the request to the Research Infrastructure Provider (RP) existing in its country. A RP is a legal organisation, part of large Resource Infrastructures like EGI, responsible for managing and operating a number of operational services at national level supporting RCs and user communities that contribute to such RIs. The reader who is not familiar with the terms mentioned above can

[11] https://ims.egi.eu/display/EGIG/Technology+Provider
[12] https://www.egi.eu/projects/egi-ace/call-for-use-cases/

have a look at the Operations Start Guide[13] (and in our glossary) to have a complete picture of the several actors participating in our landscape.

The RP operators are going to guide and support the RC during the registration and certification procedures. First, the RC will be asked to read, understand, and accept:

- the “RCs Operational Level Agreement”[14], an agreement made between the RC and its RP that defines the minimum set of operational services and the respective quality parameters that a Resource Centre is required to provide in EGI;
- the Security Policies[15] defined in EGI to guarantee that all the security aspects with the service delivery are fulfilled and enforced.

The next step is registering the RC in the EGI Configuration Database[16]: the provided information, from the generic contacts and roles of people to the service endpoints details will be needed to trigger the daily operations of other services and activities provided by the EGI Infrastructure such as the Monitoring of the resources, the Accounting, the Support, and the security activities.

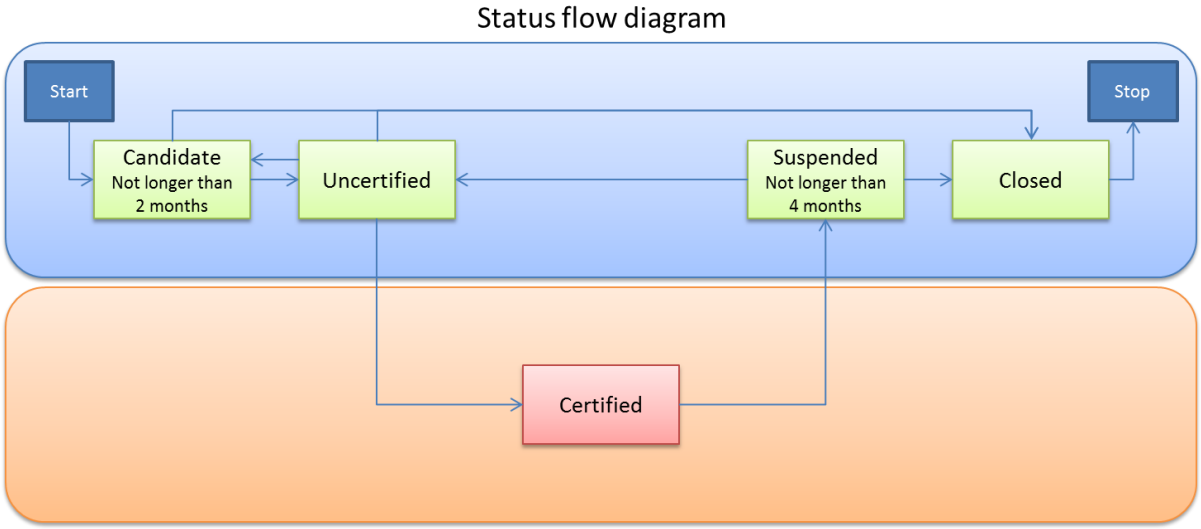

Figure 2. Diagram of the RCs status flow.

Once the entry in the Configuration Database is complete, the RP changes the RC status from “Candidate” to “Uncertified” (Fig. 2), and the certification procedure can start: it comprises a series of technical controls to verify that the provided services work according to the expectations in the RC OLA. Any identified issue is notified by the RP operators to the RC and investigated until its solution.

When all the certification controls are successfully passed, the RC status is changed to “Certified” meaning that the RC is included in the production infrastructure and its resources can be consumed by the users of the infrastructure (see next section).

[13] https://docs.egi.eu/providers/getting-started/operations_start_guide/
[14] https://documents.egi.eu/document/31
[15] https://confluence.egi.eu/display/EGIPP/EGI+Federation-wide+Information+Security+policies
[16] https://goc.egi.eu/

3.1.2 Setting up agreements with customers

Once moved to the production infrastructure, a RC is ready to deliver its resources to any of the users' communities consuming the infrastructure. Here the Service Level Management (SLM) process intervenes as a matchmaker between service expectations and needs of the Virtual Organisations (VOs)[17] and the capabilities of the RCs. During the selection of the providers for service provisioning, technical requirements collected from the customer are used by EGI to launch a call open to all of the providers. The Expression of Interests (EoIs) collected during the negotiation phase will be used to identify the provider(s) that best match the customer's requirements and expectations. From a technical perspective, several aspects will be considered during the negotiation phase including the geographical location of the customer, national roadmap and priority of the providers, and costs of the service provisioning in case of a pay-for-use model.

In case the negotiation phase ends positively, the selected provider(s) will:

- Define a VO Operational Level Agreement(s) (OLA) with EGI Foundation for providing the services through the EGI Portfolio to support the user community. EGI Foundation will share with the RCs a draft of the document(s) based on a predefined template and customised with the details of the specific Agreement(s), such as:
    - the main contacts to be used for communications related to the service(s);
    - the duration of the Agreement;
    - conditions for operating the service (service hours and exceptions);
    - Service Level Targets;
    - if the resources are exclusively allocated or are subject to local availability;
    - the payment mode;
    - responsibility in case of violations and complaints;
    - any limitations and constraints (if any);
    - the frequency of service performance reports.
- Configure the service(s) in the scope of the Agreement(s) enabling the support of the Customer's VO and activating the monitoring of the services/resources.

At the same time, EGI Foundation sets up a VO Service Level Agreement (SLA) with the given user community for the provisioning of the requested service. The EGI VO SLA is secured with related EGI VO OLAs and is agreed on a case-by-case basis (Fig.3).

[17] https://confluence.egi.eu/display/EGIG/Virtual+organisation

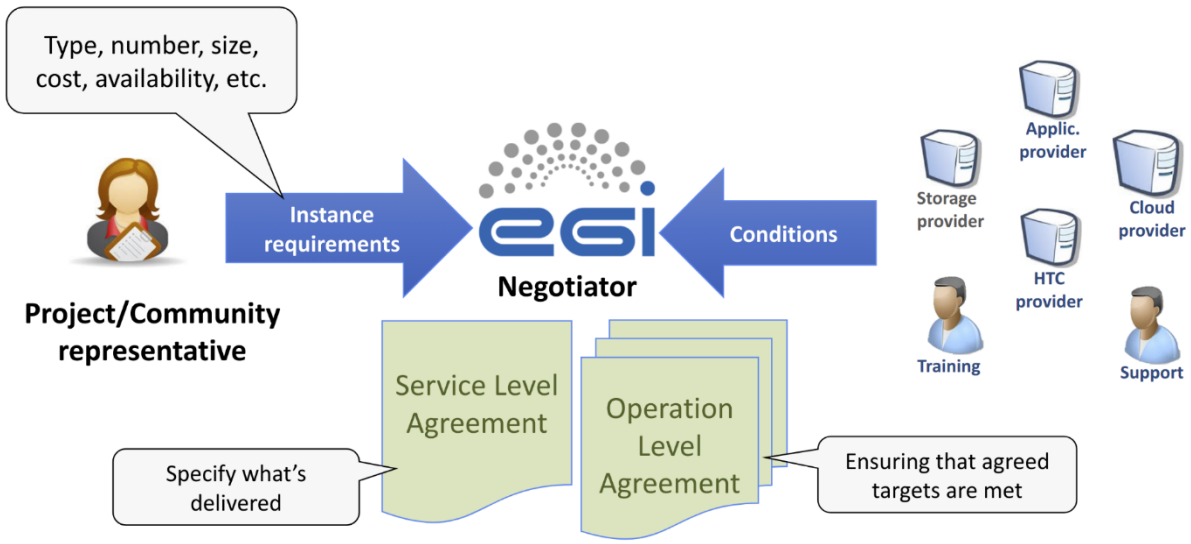

Figure 3. Relationship between SLA and OLA

Once approved, the Agreement is automatically renewed, as long as the provider(s) does (do) not express a decision to terminate the Agreement at least a month before the expiration date. In case of termination of the Agreement, the provider must remove the support of the customer. The Agreement can also be terminated by the customer.

3.1.3 Managing service orders

Customers can request access to the services of the EOSC Compute Platform through the EOSC Portal Marketplace. Access to the services is either fully open, or behind service-specific authentication and authorisation steps.

Depending on the nature of the service ordered, different levels of technical support are requested to the service providers including the activation of a new Virtual Organisation (VO), or the customization of the service with dedicated set-up to meet the customer's expectations. Service providers receive notifications about services orders via SOMBO[18] and with the support and oversight of the EGI Foundation they deal with them.

3.1.4 Incidents and service requests

Providing support is a fundamental part of the daily activity of a provider participating in a large research infrastructure like EGI. The support is meant not only towards the users accessing the resources but also towards those who are involved in the management and oversight of the infrastructure. As defined in the RC OLA, the RC will handle incidents[19] and service requests[20] registered as tickets in the EGI Helpdesk service, with the expectation to acknowledge and process any notified issue within the agreed response time associated with the priority of the ticket. The response time is defined by the Quality of Support levels[21], and for the RCs the level will be Medium, meaning that there will 4 priorities for the incidents

[18] https://opsportal.eosc-portal.eu/login/
[19] https://confluence.egi.eu/display/EGIG/Incident
[20] https://confluence.egi.eu/display/EGIG/Service+request
[21] https://confluence.egi.eu/display/EGISLM/Service+Level+Target+-+Quality+of+Support

(requiring for example up to 5 working days for the “less urgent” tickets and up to 1 working day for the “top priority” ones), while any service request will be processed as “less urgent” ticket.

3.1.5 Performance reports: enforcing OLAs

As defined in the RCs OLA, the performance of the delivered services should meet the Service Level Targets: the monthly performance of the RCs is monitored, and when the targets are not achieved for three consecutive months, the affected RCs are notified through a ticket about the OLA violation and requested to provide within 10 working days an explanation for the low performance and a plan for improvement. The RCs not providing a satisfactory explanation or not replying at all are eligible for suspension. In order to re-join the EGI Infrastructure, any suspended RC should undergo a new certification procedure. The “Suspended” status cannot last for more than 4 months, after which a RCs is either in production again or definitely closed (Fig. 2).

Besides the Targets defined in the RCs OLA which are enforced to guarantee the permanence of the RC in the infrastructure, also the targets promised to the users in the VO SLAs should be met on a monthly basis: also in this case, when a violation occurs, the RC is requested to provide a justification and a plan for improving the quality of the provided services. If repeated violations occur, the SLA can be renegotiated with the customer, either by changing the Service Level Targets, or by choosing a different RCs as a provider.

3.1.6 Dealing with security incidents and vulnerabilities

The security activities are coordinated by several teams working together and presented in section 4.6 describing the ISM process.

The security posture of the infrastructure is framed by the set of policies constituting the **Security Policies**[22]. Those policies cover different complementary activities including the operation of services, the processing of personal data and the management of security incidents and vulnerabilities. Those two aspects are presented in more detail in this section.

3.1.6.1 Dealing with security incidents

The **Security Incident Response Policy**[23] aims at ensuring that all incidents are investigated as fully as possible, and that Resource Centres promptly report intrusions. In particular, security incidents are to be treated as serious matters and their investigation must be resourced appropriately.

In case of the suspected security incidents, Resources Centres report it to their Operations Centre Security Officer and to EGI Computer Security Incident Response Team (CSIRT) within 4 hours of discovery.

This initial step will start the coordination of the incident response as documented in the procedure **SEC01 EGI CSIRT Security Incident Handling Procedure**[24]. This procedure

[22] https://go.egi.eu/security-policies
[23] https://go.egi.eu/security-incident-response-policy
[24] https://go.egi.eu/sec01

has been implemented according to the Security Incident Response Policy, to minimise the impact of security incidents affecting the Resource Centres part of the infrastructure. This procedure covers guidance on how the incident response should be coordinated, describing the responsibilities of the various parties, and encourages post-mortem analysis and promotes cooperation between Resource Centres.

3.1.6.2 Handling of vulnerabilities

The handling of vulnerabilities is a very formal process involving many different entities, as presented below.

Anyone can report a software vulnerability via a form[25] or by email contacting the Software Vulnerability Group.

The report will trigger an assessment, following the **SEC02 Software Vulnerability Issue Handling**[26] procedure, by the Software Vulnerability Group (SVG), of the risk level associated with this vulnerability in the context of the activities of the EGI Infrastructure.

Once a vulnerability has been identified as presenting a risk to the infrastructure, it will be decided if an advisory should be prepared and circulated to the security contacts of the sites. After an agreed period of time and depending on their confidentiality, advisories are made public.

Vulnerabilities identified as critical are handled according to the procedure **SEC03 EGI-CSIRT Critical Vulnerability Handling**[27]. When applicable, this usually involves developing a custom security monitoring probe[28] created to identify on High Throughput Compute RCs if their resources are vulnerable to the vulnerability. The status is closely monitored by the security team and accessible to the affected RCs.

Using this information correlated with the one from Pakiti[29] (the patch management service collecting information about the patches deployed at the various High Throughput Compute RCs), the Incident Response Task Force (IRTF) on duty security officer will open tickets against the impacted sites according to the **WI07 Security Vulnerability Handling**[30] procedure.

The EGI Service Delivery and Information Security (SDIS) team of the EGI Foundation will follow up with the resource provider to work on resolving the ticket. The first duty of the resource provider is to acknowledge the vulnerability and then work on a prompt resolution as suggested in the ticket. In case a satisfactory resolution is not reached in due time, or a sign of active progress on addressing the vulnerability is not visible, the specific resource centre may be suspended.

---

[25] https://csirt.egi.eu/report-vulnerability/
[26] https://go.egi.eu/sec02
[27] https://go.egi.eu/sec03
[28] https://github.com/ARGOeu/secmon-probes/
[29] https://pakiti.egi.eu/
[30] https://go.egi.eu/wi07

3.2 Technology Providers (TPs)

Technology Providers develop or deliver technology and software for specific user communities or customisation for specific requirements. In our case, they maintain the middleware which the RCs install and that allows the users to exploit the compute, storage, data, and cloud resources.

3.2.1 Integration of middleware stack

To assure production quality of the EGI Infrastructure, every middleware stack (Compute, Storage, etc.) installed on and delivered by the RCs needs to fulfil a number of requirements.

For this purpose a procedure[31] was defined to ensure that any single aspect of the integration of the new piece of middleware with the infrastructure is covered before the conclusion of the process.

After the creation of the request in the EGI Helpdesk[32], with details about the technology, the contacts, the expected customers, and the motivation, the integration steps cover the following areas (where possible, steps can be done in parallel):

- Underpinning Agreement (UA)[33] between EGI Foundation and the technology provider
    - it could be either the "Corporate-level Technology Provider Underpinning Agreement[34] or a customised version.
- Configuration Management: mapping of the new technology in the Configuration Management Database (CMDB)
- Information System: evaluating if the new technology should publish information in the Information System according to the GLUE Schema[35].
- Monitoring: the new technology should allow external monitoring. If particular aspects of the technology need to be monitored, specific monitoring probes should be provided by the TPs and deployed on the EGI Monitoring service[36].
- Support: the Support Unit where incidents and service requests will be addressed needs to be defined in the EGI Helpdesk, associated to the Quality of Support[37] defined in the UA.
- Accounting: the need to gather usage data, which depends on the technology itself and on the infrastructure requirements and will be published in the EGI Accounting Portal[38].

[31] https://confluence.egi.eu/display/EGIPP/PROC19+Integration+of+new+cloud+management+framework+or+middleware+stack+in+the+EGI+Infrastructure
[32] https://helpdesk.egi.eu/
[33] https://ims.egi.eu/display/EGIG/Underpinning+agreement
[34] https://documents.egi.eu/document/2589
[35] GLUE Specification v. 2.0: http://www.ogf.org/documents/GFD.147.pdf
[36] https://argo.egi.eu/
[37] https://confluence.egi.eu/display/EGISLM/Service+Level+Target+-+Quality+of+Support
[38] https://accounting.egi.eu/

- Integration in UMD: the Unified Middleware Distribution is the integrated set of software components contributed by Technology Providers and packaged for deployment as production quality services in EGI.
- Documentation: exhaustive documentation for RC administrators and users should be provided and may be added to the EGI Documentation[39].
- Security: a security assessment of the software is required according to a number of guidelines defined by the EGI Security team.

3.3 EGI Foundation services in 'Compute and Data Federation' or 'Platform services'

Services in this group include Check-in, DataHub, Data Transfer (FTS), Notebooks, Workload Manager.

To become a provider of one of these services you first have to become provider of an EGI Foundation service within the 'federated resources' block. (i.e. follow Section 3.1). Once such a foundational role is fulfilled you can configure/deploy the additional service within your resource centre. This pre-requirement typically requires you to become an EGI Cloud service provider, i.e. deploy OpenStack and federate it into the EGI Cloud Compute service.

3.4 Non-EGI Foundation services in 'Compute and Data Federation' or 'Platform services'

Services in this group include AppDB, Infrastructure Manager, OpenRDM, CVMFS, RUCIO, EC3, DODAS, Indigo PaaS Orchestrator, DEEP training solution, Binder.

The same rule applies as for the previous Group of Section 3.3: To become a provider of one of these services you first have to become provider of an EGI Foundation service within the 'federated resources' block. (i.e. follow Section 3.1). Once such a foundational role is fulfilled you can configure/deploy the additional service within your resource centre. This pre-requirement typically requires you to become an EGI Cloud service provider, i.e. deploy OpenStack and federate it into the EGI Cloud Compute service.

3.5 Central services enabling the EGI federation

With the term "central" or "core service" we refer to a category of services in the EOSC Compute Platform (like the service management tools and the services mentioned in section 3) providing capabilities that support the other services of the infrastructure and the related activities. They are delivered through a single instance (with the fail-over and high-availability mechanisms deemed necessary), and differently from services with a distributed nature such as HTC, Cloud, and Storage, they cannot be ordered through the Marketplace, but they become available as soon as a user joins the infrastructure (e.g., the access to the EGI Helpdesk service).

[39] https://docs.egi.eu/

3.5.1 Selection of the providers and registration

When a service is co-funded by EGI Foundation, which usually covers part of the funding associated to a given international project, the providers are selected through a bidding process: a call of expression of interest is announced and advertised to the EGI Council[40] containing the technical details of the services that should be delivered and then any provider who is an EGI Participant[41] can apply to the bid.

With the selected providers, EGI Foundation negotiate and sign an OLA defining terms and conditions for the delivery of the services, starting the process within Service Portfolio Management (SPM) to add them to the EGI Service portfolio[42] if not already included. At this point, similar steps to the ones for resource and technology providers follow in order to guarantee the regular day-to-day operation of the service, such as:

- registration in the Configuration Database and certification;
- definition of the Support Unit in the helpdesk system to handle incidents and service requests;
- enabling of the monitoring;
- periodic performance reports as defined in the given OLA to verify that the Service Level Targets are achieved.

In addition to this, the providers are also requested to create a capacity plan, an availability and continuity plan, and to interact with Change Management (CHM) and Release and Deployment Management (RDM) processes for managing changes and new releases of their services.

3.5.2 Capacity plan

The capacity plan is important to assess if the capacity of the service is sufficient to respond to the current and to the future demand of the service. Any capacity aspect of the service delivery is analysed (human, technical, and financial) with the definition of quantitative parameters to measure the usage and the load of the service. The approach to adjust the capacity of the service in relation to a change in the demand is defined and recommendations on capacity requirements for the next reporting period are provided as well.

EGI Foundation defined a template for the Capacity plans and will contact and support the service providers either for the creation of a new Capacity plan or for the review of an existing one (the reviews are usually performed at least twice per year).

3.5.3 Availability and continuity plan

In the Availability and Continuity plan a number of risks affecting the availability and continuity of the service is identified and assessed: each risk is rated in terms of likelihood and impact with the definition of countermeasures to implement that should avoid the occurrence of the given risk. Any remaining vulnerability is identified as well, and in case the

[40] https://ims.egi.eu/display/EGIG/EGI+Council
[41] https://ims.egi.eu/display/EGIG/EGI+Participant
[42] https://www.egi.eu/services/

rating of a risk is considered to be too high in relation to the risk acceptance criteria, a plan either to improve the existing countermeasures or to implement new ones is created, with the aim either to reduce the likelihood of a risk or to mitigate the impact in case a risk occurs.

The plan is completed by a continuity and recovery test, where the continuity of the service and its recovery capacity are tested against a simulated disruption scenario: the performance of this test is useful to spot any issue in the recovery procedures of the service.

Also in this case, the discussion of the Availability and Continuity plan is started and overseen by EGI Foundation who shares with the providers a template that will be filled in with the details of the given service. Availability and Continuity plans are reviewed on a yearly basis.

3.5.4 Managing changes and new releases

All changes to the services should be managed by the EGI Change Management (CHM) process according to the Change Policy[43] in order to evaluate the potential impact that a change can have on the service itself and on the infrastructure as a whole. When registering a Request for Change, besides a general description of the change, the providers are expected to provide: the risk level as a result of assessing the impact and the likelihood of things going wrong, the type of change, the eventual list of other services potentially affected by the change, if it is possible to revert the change, the proposed date for the implementation of the change, and if it is needed to schedule a downtime of the service. Requests for Changes are assessed by the Change Advisory Board (CAB), and then decided whether the Change is going to be approved or rejected.

For the recurrent changes with a relatively low risk level, the providers can request to classify them as Standard Changes, so that invoking the CAB won't be necessary and they can undergo the release process after the release plan is agreed with CHM staff. The Emergency Changes are created when there is an urgent need to fix either a newly discovered security vulnerability or a critical issue: also in this case the formal approval of the CAB is not required but it is enough that the release plan is accepted by CHM staff. In all of the other situations the changes are classified as Normal and depending on their risk level they might need to be assessed by the CAB.

Before the release in the production environment, the providers invite the users to test the new changes on a pre-production instance in order to gather feedback and to find out possible issues that might be overlooked during the preparation of the new release. If no problems are found, the release can go live, and a Post-Implementation Review is conducted after a few days to close the case.

3.5.5 Security aspects

The providers of central services are subject to the same policies, procedures and requirements applied to the federated service providers, previously documented in section 3.1.6.

[43] https://confluence.egi.eu/display/EGIPP/Change+management+policy

Nevertheless, they are also subject to the following requirement that is documented in the service Operational Level Agreement (OLA) that is being agreed with them:

- They should immediately report suspected security incidents to the EGI Foundation. This is not exempting them to follow the **SEC01 EGI CSIRT Security Incident Handling Procedure**[44] and inform EGI CSIRT within 4 hours.

It's also important to understand that when processing of personal data is taking place, EGI Foundation holds the role of Data Controller and the provider is a Data Processor, as defined in the Global Data Protection Regulation (GDPR)[45]. Data Processing Agreements, regulating the conditions and constraints of the data processing activities conducted by the Data Processor on behalf of the Data controller, will be put in place on the initiative of the EGI Foundation staff. EGI Foundation will also prepare, together with the central service provider, adequate Privacy and Acceptable Use policies that have to be presented and made available to the users of the service. EGI Foundation is also complying with all the principles set out by the GÉANT Data Protection Code of Conduct in its more recent version, implying that the central service provider should also comply with them.

The central service provider should also follow requirements relating to the software and covering the usage of a proper licence, the access to and management of the source code, implementation of best practices; as well as requirements relating to the IT Service management and covering the need for having key staff properly trained about IT Service Management, committing to continual improvement and having their Service Management System (SMS) interfacing with the EGI Service Management System, especially for important processes like the Change Management process.

3.6 New services in the EOSC Compute Platform

The EOSC Compute Platform is currently linked to the EGI Governance, and services of the ECP are contributed by the EGI Council members. These members can propose new services through the EGI Service Strategy, that defines the overall direction to EGI services for a few-year time window. The services are designed, validated through the EGI Community, with the help of the EGI Services and Solutions Board (SSB).

[44] https://go.egi.eu/sec01
[45] https://gdpr.eu/article-4-definitions/

4. EGI Foundation Service Management System (SMS)

4.1 What is an IT Service Management System?

The key idea behind IT service management could be summarised 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. A Service Management System is the overall management system that controls and supports management of services within an organisation or federation. The SMS can be regarded as the entirety of interconnected policies, processes, procedures, roles, agreements, plans, related resources and other elements needed and used by a service provider to effectively manage the delivery of services to customers. By following the processes of the SMS the activities carried out to plan, deliver, operate and control the services become more structured and repeatable, with clearly defined responsibilities. All this helps an IT organisation to increase its level of professionalism and organisational maturity.

4.2 Service Portfolio Management (SPM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR1.1 A service portfolio shall be maintained. All services shall be specified as part of the service portfolio. • PR1.2 Design and transition of new or changed services shall be planned. • PR1.3 Plans for the design and transition of new or changed services shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria. • PR1.4 The organisational structure supporting the delivery of services shall be identified, including a potential federation structure as well as contact points for all parties involved. • PR2.1 A service catalogue shall be maintained.
ISO20k 2018 additional requirements
• A service portfolio is used to manage the entire lifecycle of all services including proposed services, those in development, live services defined in the service catalogue(s) and services that are to be removed. • Service requirements for existing services, new services and changes to services shall be determined and documented • Propose changes where needed to align the services with the service management policy, service management objectives and service requirements, taking into consideration known limitations and risks • Prioritise requests for change and proposals for new or changed services to align with business needs and service management objectives, taking into consideration available resources • Coordinate activities with other parties involved in the service lifecycle • Determine the criticality of services based on the needs of the organisation, customers, users and other interested parties

- Determine and manage dependencies and duplication between services
- Determine current demand and forecast future demand for services
- Monitor and report on demand and consumption of Services
- The catalogue of services shall include the dependencies between services and service components.
- Provide access to appropriate parts of the service catalogue(s) to its customers, users and other interested parties.

The purpose of Service Portfolio Management is to create, manage and improve a service portfolio containing a detailed design package for each IT service.

In a Federated environment as well as a project context, the benefit of having a common SPM is evident in managing the services through common standards, terms of use, procedures, documentation and communications.

The most important concepts are related to control the services in their lifecycle, to properly track any impacting change, new entry or retiring, recording the evolution of any item of the portfolio through the various maturity status also called service phases (alpha, beta, production, etc.)

The preparation of a full Service Design and Transition Package (SDTP) ensures that nothing is missed, and the service is ready to be offered in any Customer-oriented catalogue. An SDTP consists of a number of documented plans and other relevant information, available in different formats, including e.g.:

- a list of requirements and service acceptance criteria;
- capacity, availability, and continuity plans;
- communication and training plans;
- technical plans and specifications.

The management of the Portfolio is strictly connected with the management of changes, highlighting the importance of a correct impact analysis in the major change planning, in order to ensure the continuity of the services, avoiding any unexpected disruption.

Another important approach to follow is to implement through procedures a way of working able to fully manage the updates and changes to services.

The SPM Procedures support the review of the full Portfolio in terms of objectives and scope too, and to propose organisational model changes necessary to support the development and delivery of the new services.

Recently, our SPM process has started to also maintain the Service Catalogue, taking over the requirement (PR2.1) that originally was under SLM responsibility.

4.3 Service Level Management (SLM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)

- PR2.2 For all services delivered to customers, SLAs shall be in place.
- PR2.3 SLAs shall be reviewed at planned intervals.
- PR2.4 Service performance shall be evaluated against service targets defined in SLAs.

• PR2.5 For supporting services or service components provided by federation members or groups belonging to the same organisation as the service provider or external suppliers, OLAs and UAs shall be agreed. • PR2.6 OLAs and UAs shall be reviewed at planned intervals. • PR2.7 Performance of service components shall be evaluated against operational targets defined in OLAs and UAs.
ISO20k 2018 additional requirements
• Ensure that changes to documented service requirements, the service catalogue, SLAs and other documented agreements are controlled by the change management process. • Monitor, review and report on actual and periodic changes in workload compared to workload limits in the SLAs.

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. Performance reports are produced in collaboration with Service Availability and Continuity Management (SACM) and Supplier Management (SUPPM) to verify that the Service Level Targets are achieved as expected; violations to the agreements are dealt with according to the definition in the related agreement.

4.4 Service Reporting Management (SRM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR3.1 Service reports shall be specified and agreed with their recipients. • PR3.2 The specification of each service report shall include its identity, purpose, audience, frequency, content, format and method of delivery. • PR3.3 Service reports shall be produced. Service reporting shall include performance against agreed targets, information about significant events and detected nonconformities.
ISO20k 2018 additional requirements

• Ensure that decisions are made, and actions taken based on the findings in service reports. Ensure that agreed actions are communicated to interested parties.
• Ensure that service reporting covers:
  ○ information about major incidents, deployment of new or changed services and the service continuity plan being invoked
  ○ workload characteristics including volumes and periodic changes in workload
  ○ trend information
  ○ information about customer satisfaction and service complaints
• Determine reporting requirements

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

and whenever a non-conformity concerning a report definition is spotted, a list of actions is undertaken to fix the inconsistency in the report.

4.5 Service Availability and Continuity Management (SACM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
● PR4.1 Service availability and continuity requirements shall be identified taking into consideration SLAs. ● PR4.2 Service availability and continuity plans shall be created and maintained. ● PR4.3 Service availability and continuity planning shall consider measures to reduce the probability and impact of identified availability and continuity risks. ● PR4.4 Availability of services and service components shall be monitored.
ISO20k 2018 additional requirements
● Ensure that changes to the service availability and continuity plans are controlled by the change management process. ● Ensure that service continuity plans, contact lists and the CMDB are accessible when access to normal service locations is prevented. ● Ensure that service availability and continuity plans are tested against the availability and continuity requirements and re-tested after major changes to the service environment. ● Additional elements to be included in or referenced from service continuity plans: ○ procedures to be implemented in the event of a major loss of service, or reference to them ○ availability targets when the plan is invoked ○ recovery requirements ○ approach for the return to normal working conditions

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 Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) and the availability needs in general, and that an adequate level of service continuity is guaranteed in case of exceptional events.

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

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

The result of these activities is the creation of a Service Availability and Continuity Plan covering the definition and planning of the measures needed to be implemented in order to reduce the probability and the impact of the identified availability and continuity risks. The

plan should also comprise an availability and continuity test to verify the robustness of the adopted measures and of the service recovery procedures.

4.6 Capacity Management (CAPM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
● PR5.1 Service capacity and performance requirements shall be identified taking into consideration SLAs. ● PR5.2 Capacity plans shall be created and maintained. ● PR5.3 Capacity planning shall consider human, technical and financial resources. ● PR5.4 Performance of services and service components shall be monitored based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.
ISO20k 2018 additional requirements
● Ensure that changes to the capacity plans are controlled by the change management process. ● Additional elements to be included in or referenced from capacity plans: ○ current and forecast demand for services ○ expected impact of agreed requirements for availability, service continuity and service levels ○ timescales, thresholds and costs for upgrades to service capacity

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

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

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

4.7 Information Security Management (ISM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
● PR6.1 Information security policies shall be defined. ● PR6.2 Physical, technical and organisational information security controls shall be implemented to reduce the probability and impact of identified information security risks. ● PR6.3 Information security policies and controls shall be reviewed at planned intervals. ● PR6.4 Information security events and incidents shall be given an appropriate priority and managed accordingly.

• PR6.5 Access control, including provisioning of access rights, for information-processing systems and services shall be carried out in a consistent manner.
ISO20k 2018 additional requirements
• Ensure that internal information security audits are conducted and that audit results are reviewed to identify opportunities for improvement. • Ensure that the approach to information security risk management and the criteria for accepting risks are defined. • Ensure that the risks to which information security controls relate are described as part of the documentation of these controls. • Ensure that information security controls with external organisations that have a need to access, use or manage the service provider's information or services are documented, agreed and implemented.

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

The ISM process aims at addressing different needs by performing the following activities:

- Managing the security aspects of the daily activities of the EGI Foundation employees by providing relevant policies (like the ICT Policy) and procedures (like for managing access rights for the new employees, managing the EGI Foundation's assets and related controls, risks and security incidents ...)
- Managing activities related to Data Protection (maintaining the directory of the processing activities, preparing service-specific privacy policies, managing Data Processing Agreements,...)
- Liaising with the activities devoted to the EGI Federation security teams, like the ones related to infrastructure policies, software vulnerability assessment or handling and the incident response.

The coordination of the security of the EGI infrastructure is since ever taken care by a set of interrelated and interdependent security teams, building on the knowledge and expertise of the federation participants:

- The EGI Security Policy Group (SPG)[46] develops policies covering diverse aspects, including operational policies (agreements on vulnerability management, intrusion detection and prevention, regulation of access, and enforcement), incident response policies (governing the exchange of information and expected actions), participant responsibilities (including acceptable use policies, identifying users and managing user communities), traceability, legal aspects, and the protection of personal data. The prepared policies are to be adopted by the EGI Federation management.

[46] https://go.egi.eu/spg

- The EGI Software Vulnerability Group (SVG)[47] aims to eliminate existing software vulnerabilities from the deployed infrastructure and prevent the introduction of new ones and runs a process for handling software vulnerabilities reported. SVG issues advisories whenever a software vulnerability has been identified as causing a risk to the activities of the infrastructure.
- The EGI Computer Security Incident Response Team (CSIRT)[48] coordinates operational security activities within the EGI Infrastructure to deliver a secure and stable infrastructure, giving scientists and researchers the protection and confidence they require to carry out their research safely and effectively.

In addition to those teams, the EGI Service Delivery and Information Security (SDIS) team, previously known as the EGI Operations team, is responsible for liaising with the Federation participants to ensure they are aware of the policies and to follow up with the handling of the vulnerability identified by the SVG and reported to the affected sites by the CSIRT.

While the ISM process was initially scoped on the activities of the EGI Foundation team, leaving the aspects related to the EGI Federation to the aforementioned teams, the ISM scope is now clearly covering all the services provided in the catalogue and thus needs to coordinate with the security teams.

There is an ongoing process of incorporating the existing activities with the ISM process, like linking the security policies and procedures to the ISM process[49]. This consolidation is to be strengthened in the context of the EGI-ACE project.

4.8 Customers Relationship Management (CRM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR7.1 Service customers shall be identified. • PR7.2 For each customer, there shall be a designated contact responsible for managing the customer relationship and customer satisfaction. • PR7.3 Communication mechanisms with customers shall be established. • PR7.4 Service reviews with the customers shall be conducted at planned intervals. • PR7.5 Service complaints from customers shall be managed. • PR7.6 Customer satisfaction shall be managed.
ISO20k 2018 additional requirements
• Ensure that changes to documented service requirements are controlled by the change management process. • Ensure that the definition of a service complaint is agreed with the customer.

Customer Relationship Management (CRM) provides the policies and the procedures to identify and analyse potential new customers, partnerships and business opportunities, turn prospective opportunities into active customers/partners, supporting the customers in reaching long-term operational setups at EGI Service Providers, maintain good relationships

[47] https://go.egi.eu/svg
[48] https://csirt.egi.eu
[49] https://go.egi.eu/ism

with active customers, and the services order management for handling service orders requests from end-users submitted via the EOSC Portal Marketplace.

Depending on the scope of the envisaged collaboration the opportunities must be tracked in one of these two Databases, depending on the scope of the envisaged collaboration:

- Customer Database
- Partnership Opportunity Database

Suggestions for improvements collected during the interviews with customers are collected in the Customer Satisfaction and Service Review Database.

4.9 Suppliers relationship Management (SUPPM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR8.1 Suppliers shall be identified. • PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with the supplier. • PR8.3 Communication mechanisms with suppliers shall be established. • PR8.4 Supplier performance shall be monitored.
ISO20k 2018 additional requirements
• Ensure that roles of, and relationships between, lead and sub-contracted suppliers are documented. Verify that lead suppliers are managing their sub-contracted suppliers to fulfil contractual obligations. • Ensure that changes to contracts with suppliers are assessed for the impact of the change on the SMS and the services before approval • Ensure that the contracts with suppliers reflect current requirements.

Suppliers Relationship Management (SUPPM) ensures that a healthy relationship with the suppliers is maintained and that they are supported in delivering services to customers. The suppliers are registered in a database with associated contacts, services delivered, and related agreements. The suppliers' performance is periodically monitored according to the conditions defined in the agreement for the provision of the service the given supplier is involved in. An important task of this process is also the management of the bidding process for the selection of suppliers of the central services that will support the activities of the EGI Federation, as already explained in section 3.3.1.

4.10 Incident and Service Request Management (ISRM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR9.1 All incidents and service requests shall be registered, classified and prioritised in a consistent manner. • PR9.2 Prioritisation of incidents and service requests shall consider service targets from SLAs. • PR9.3 Escalation of incidents and service requests shall be carried out in a consistent manner. • PR9.4 Closure of incidents and service requests shall be carried out in a consistent manner.

• PR9.5 Personnel involved in the incident and service request management process shall have access to relevant information including known errors, workarounds, configuration and release information. • PR9.6 Users shall be kept informed of the progress of incidents and service requests they have reported. • PR9.7 There shall be a definition of major incidents and a consistent approach to managing them.
ISO20k 2018 additional requirements
• When prioritising incidents and service requests, ensure that the impact and urgency of the incident or service request are taken into consideration. • Ensure that top management is informed of major incidents, and a designated individual responsible for managing the major incident is appointed. After the agreed service has been restored, ensure that a major incident review is performed to identify opportunities for improvement.

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

With the EGI Helpdesk system any registered user of our infrastructure can create either an incident or a service request which is addressed to and followed-up by the supporters of the affected service of our catalogue. The 3 levels of support ensure that:

- an initial analysis of the incoming ticket is performed;
- configuration and deployment issues as well as suspected software defects are properly dealt with;
- fixes to confirmed software bugs are worked on, and requests of new features are properly evaluated and implemented.

Major incidents are properly classified and managed with the involvement of the relevant team of experts to assess the status of the impacted services, evaluate the possible solutions and workarounds with the corresponding time resolution estimations.

4.11 Problem Management (PM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR10.1 Problems shall be identified and registered based on analysing trends on incidents. • PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on the services. • PR10.3 If a problem is not permanently resolved, a known error shall be registered together with actions such as effective workarounds and temporary fixes. • PR10.4 Up-to-date information on known errors and effective workarounds shall be maintained.
ISO20k 2018 additional requirements

- Ensure that problems requiring changes to a CI are resolved according to the change management policy.
- Ensure that the effectiveness of problem resolution is monitored, reviewed and reported.
- Resolve problems if possible.

The main objective of Problem Management (PM) is to investigate the root causes of incidents in order to avoid future recurrence of incidents by resolving the underlying causes, or to ensure that workarounds or fixes are available within the services provided by the EGI Infrastructure.

The identified problems are registered in a Known Error Database (KEDB), reporting related workarounds until a definitive solution is provided.

4.12 Configuration Management (CONFM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)

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

ISO20k 2018 additional requirements

- Ensure that the information from the CMDB is provided to the change management process, to support the assessment of requests for changes.
- Ensure that the information recorded for each CI include at least:
  - description of the CI
  - relationship(s) between the CI and other CIs
  - relationship(s) between the CI and service components
  - status
  - version
  - location
  - associated requests for changes
  - associated problems / known errors

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

Our Configuration Management Database (CMDB) is composed by two parts: an Internal CMDB created with the purpose to manage the CIs that are in the scope of CHM and RDM processes; and a federated CMDB for the CIs controlled at the Infrastructure level with

specific procedures regulating registration and decommission of services, their oversight, monitoring and support, and their security aspects.

4.13 Change Management (CHM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
● PR12.1 All changes shall be registered and classified in a consistent manner. ● PR12.2 All changes shall be assessed and approved in a consistent manner. ● PR12.3 All changes shall be subject to a post implementation review and closed in a consistent manner. ● PR12.4 There shall be a definition of emergency changes and a consistent approach to managing them. ● PR12.5 In making decisions on the acceptance of requests for change, the benefits, risks, potential impact to services and customers and technical feasibility shall be taken into consideration. ● PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes, and proposed deployment dates, which shall be communicated to interested parties. ● PR12.7 For changes of high impact or high risk, the steps required to reverse an unsuccessful change or remedy any negative effects shall be planned and tested.
ISO20k 2018 additional requirements
● Ensure that a change management policy is established that defines: ○ CIs which are under the control of change management ○ criteria to determine changes with potential to have a major impact on services or the customer. ● Ensure that the removal of a service and transfer of a service from the service provider to the customer or a different party are classified as a change with the potential to have a major impact. ● Ensure that requests for changes are analysed at planned intervals to detect trends. Ensure that the results and conclusions drawn from the analysis are recorded and reviewed to identify opportunities for improvement. ● Consider the potential impact of each change on: ○ services ○ customers, users and other interested parties ○ policies and plans ○ capacity ○ service availability ○ service continuity ○ information security ○ other requests for change ○ releases and plans for deployment

The purpose of Change Management (CHM) is to ensure that changes to Configuration Items are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services. All changes are registered along with a risk level as an outcome of the Impact and Likelihood of the change

going wrong and are evaluated by the Change Advisory Board (CAB) to get the approval. The recurrent changes with a relatively low risk rating can be classified as Standard Changes the first time they are evaluated by the CAB, and they do not require a new approval by the CAB the next time they occur. The CAB also performs a Post-Implementation Review of the changes to verify that no problem arises after the release of the changes.

4.14 Release and Deployment Management (RDM)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)
• PR13.1 A release policy shall be defined. • PR13.2 The deployment of new or changed services and service components to the live environment shall be planned with all relevant parties including affected customers. • PR13.3 Releases shall be built and tested prior to being deployed. • PR13.4 Acceptance criteria for each release shall be agreed with the customers and any other relevant parties. Before deployment, the release shall be verified against the agreed acceptance criteria and approved. • PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers. • PR13.6 Releases shall be evaluated for success or failure.
ISO20k 2018 additional requirements
• Ensure that the definition of an emergency release is agreed with the customer. • Ensure that the release policy is agreed with customers and states the frequency and types of releases. • Ensure that release planning is coordinated with the change management process and includes references to the related requests for changes, and problems / known errors which are being closed through the release. • Ensure that a controlled acceptance test environment is used for the building and testing of releases. • Ensure that incidents related to a release in the period following deployment are measured. Ensure that analysis includes an assessment of the impact of the release on the customer, and the results and conclusions drawn from the analysis are recorded and reviewed to identify opportunities for improvement. • Create a baseline of affected CIs before deployment of a release into the live environment.

Release and Deployment Management (RDM) ensures that releases are controlled and deployed in a consistent manner. This is done by ensuring a systematic approach to defining a release as a collection of one or more changes to Configuration Items that are adequately tested before being deployed to the live production environment. In collaboration with CHM, each release is reviewed after its deployment to verify its successful status.

4.15 Continual Service Improvement (CSI)

FitSM requirements (based on FitSM-1, Edition 2015, v. 2.0)

● PR14.1 Opportunities for improvement of the SMS and the services shall be identified and registered, based on service reports as well as results from measurements, assessments and audits of the SMS. ● PR14.2 Opportunities for improvement of the SMS and the services shall be evaluated in a consistent manner, and actions to address them identified. ● PR14.3 The implementation of actions for improvement of the SMS and the services shall be controlled in a consistent manner.
ISO20k 2018 additional requirements
● Ensure that opportunities for improvement are prioritised. ● Ensure that, in managing improvements, the following activities are addressed: a. setting targets for improvements in quality, value, capability, cost, productivity, resource utilisation and risk reduction. b. ensuring that approved improvements are implemented. c. revising the service management policies, plans, processes and procedures, where necessary. d. measuring implemented improvements against the targets set and, where targets are not achieved, taking necessary actions. e. reporting on implemented improvements.

The purpose of Continual Service Improvement (CSI) is to identify, prioritise, plan, implement and review improvements to services and service management. All the suggestions for improvement are properly recorded and assigned to a responsible person, and when accepted their status is periodically monitored to ensure that the implementation is achieved according to the initial plan. The process is also responsible to manage the audit plans and the review of the associated audit findings, and to schedule regular management reviews in order to periodically assess the status, the effectiveness, the efficiency, and the level of conformity of the whole SMS.

5. EGI-ACE SMS integration with EOSC Future SMS

EOSC Future operates the EOSC Service Management System (EOSC SMS), scoped on the EOSC Core, but demanding a certain level of ITSM readiness from providers of the EOSC-Exchange (thus from EGI-ACE). The EOSC SMS builds on the ITSM that was laid down by EOSC-hub[50] to ensure a robust yet pragmatic service delivery in the EOSC federated infrastructure with different types of many-to-many relationships between users, providers and clients. The EOSC SMS is structured and organised into processes and procedures according to the FitSM IT Management standard[51], i.e. the same standard that is used by EGI-ACE for the EGI Foundation services (external and internal).

At a base level, all onboarded services become in the scope of EOSC SPM when they are included into the EOSC Exchange Service Portfolio, and then publicly exposed in a Service Catalogue (the EOSC Portal and its Marketplace). How the scope of other EOSC SMS processes impacts on new onboarded services depends on the choices the service providers make for integrating with other EOSC Core services. For example, enabling 'ordering' (i.e. users have to request access to the service via the EOSC Marketplace) will bring the Exchange service partially into the scope of CRM, using the Helpdesk involves the Exchange service in the ISRM process, and so on. Additional integration activities may bring the services within the scope of other SMS processes.

As the section shows, most of the EGI-ACE services operate with a very mature SMS, and the project puts emphasis on lifting the SMS maturity of its whole portfolio.

The integration between the EGI-ACE SMS and EOSC SMS covers the areas shown in Table 2.

Table 2: Areas covered by the integration between the EGI-ACE SMS and EOSC SMS.

PROCESS IN THE EOSC SMS	INTEGRATION FROM EGI-ACE
Service Portfolio Management (SPM)	The minimum requirements of the EOSC SMS are met by any provider who successfully onboard services to the EOSC Portal. The EGI-ACE services that are onboarded to EOSC therefore already meet the EOSC Criteria.
Customer relationship management (CRM)	The order management process of EGI-ACE services is linked to the EOSC Order Management workflow. EGI-ACE participates in joint Customer engagement and support activities with EOSC Future, such as Provider Days, Ask me Anything Webinars, Joint support of ESFRI Cluster and

[50] https://www.eosc-hub.eu/eosc-hub-key-exploitable-results/#KER2
[51] FitSM IT Service Management standard: https://www.fitsm.eu/

	EOSC DIH Business Pilots.
Incident and service request management (ISRM)	EGI-ACE services use Check-in, one of the EOSC Compliant AAI Proxies. EGI-ACE CSIRT participates in the EOSC CSIRT.