D7.3: Report on the validation statistics, operational infrastructure services and recommendations for future integration work

Lead Partner:	KIT
Version:	V1.0
Status:	Draft
Dissemination Level:	Public
Document Link:	https://repository.eosc-pillar.eu/index.php/s/bymiAj5wXMN76HN

Deliverable Abstract

This deliverable describes the methodology adopted to assess the maturity level of a service and its operational readiness. The methodology was applied to a list of seventeen services part of service portfolio in EOSC-Pillar. We used a checklist template with requirements as a data collection tool. Based on the feedback received, we provide an analysis to check at what degree a service delivery is compliant to all (or to a category) the defined requirements, complemented with some important aggregation metrics. We finally propose a set of recommendations for future integration work.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 857650.

COPYRIGHT NOTICE

The EOSC-Pillar project is co-funded by the European Union Horizon 2020 programme under grant number 857650.

DELIVERY SLIP

Date	***Name***	***Partner/Activity***	***Date***
From:			
Moderated by:			
Reviewed by:			
Approved by:			

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author***
v0.1	22.09.2021	Propose a preliminary Table of Content	Lisana Berberi (KIT)
v0.2	22.10.2021	Updating TOC; adding information from the work published in MS37; Recommendation section added; add as an Annex the full table of requirements checklist and a short description of the services we collected and get feedback in order to further validate them;	Lisana Berberi (KIT)
v0.3	23.11.2021	Report some aggregation metrics as validation statistics, insert corresponding charts; internally reviewed	Lisana Berberi (KIT); reviewed by David Douard (INRIA)
v0.4	03.12.2021	Recommendation section completed. Layout format updated.	Jos van Wezel (KIT) Vincent Breton (CNRS) Lisana Berberi (KIT)
v1.0	20.12.2021	Addressed reviewers' comments.	Lisana Berberi (KIT) Jos van Wezel (KIT)

TERMINOLOGY

https://eosc-portal.eu/glossary

Terminology/Acronym	*Definition*
AAI	Authentication and Authorization Infrastructure
CTS	CoreTrustSeal
FitSM	Family of standards for lightweight IT service management
iRODS	Integrated Rule-Oriented Data System
Maturity tool	A maturity tool adopted from EOSC-Nordic project and updated as a new version from EOSC-Pillar project to assess the maturity level of service delivery.
OIDC	OpenID connect (OIDC) protocol is an identity layer built on top of the OAuth 2.0 framework. It allows third-party applications to verify the identity of the end-user and to obtain basic user profile information.
PID	A persistent identifier (PI or PID) is a long-lasting reference to a document, file, web page, or other object.
RI	Research Infrastructure
SLA	Service Level Agreement
SP	Service Provider
VM	Virtual Machine

Contents

Executive summary

This document describes the methodology adopted to assess the maturity level of services from the service delivery perspective and the outcome of our analysis of 17 services provided by EOSC-Pillar.
Our approach to assess the maturity of the services delivered in EOSC-Pillar is to require each service provider to fill a checklist template with all the defined requirements to be considered in order to deliver a good service and meet the customer's satisfaction.The maturity model assessment tool of the EOSC-Nordic regional project was used as a starting point. We added data repository requirements specific to data repository owners or managers who are offering data repository as a service. We also introduced a specific score taking only into account the positive answers to requirements considered as mandatory. As a result, our evaluation framework consists of 44 requirements regarding service management, data repository, accessibility and legal requirements, sustainability and EOSC architecture compatibility.

Our assessment tool was tested on 17 services currently provided by EOSC-Pillar partners, classified as 8 thematic services, 5 research data management services and 4 generic (common) services.
Our analysis indicates that the services achieve an overall average (64,67%) level compliance to the service delivery requirements. Hence, they already comply with most of the EOSC on-boarding validation criteria and are ready to serve a broader range of users.

1 Introduction

To assess the maturity of the services delivered in EOSC-Pillar, we propose to use a checklist template with all the defined requirements to be considered in order to deliver a good service and meet the customer's satisfaction.

We used the maturity model assessment tool [1] of the EOSC-Nordic regional project as a starting point to assess the readiness of the currently provided services in EOSC-Pillar, to be accessed and operated especially from the cross-border usage point of view. First, we reviewed the requirements of this initial version, how they were divided in five different sections and classified them into three levels: *minimum*, *intermediate,* and *high*, based on their relevance. These requirements were identified based on the FitSM[1] process for service management and the EOSC Service Description Template [2]. Next, we decided to modify this version by applying some minor changes on existing requirements and modified the classification settings to *mandatory* or *optional* instead of the original three-level based classification.

Furthermore, we added data repository requirements specific to data repository owners or managers who are offering data repository as a service. These requirements [3] are based on the latest criteria and features from different publishers and organisations (e.g., CoreTrustSeal - CTS[2], COAR[3], NIH[4], ELIXIR[5], TRUST[6]) and their respective compliance agreed on.

This tool comes as a spreadsheet with requirements designed as multiple-choice questions where service assessors can simply answer either "Yes", "No" or "N/A".

In addition to the given general score, that calculates the number of positive answers from *all the requirements*, we introduce a new specific score called custom score which counts only positive answers of *mandatory requirements* without considering optional requirements. In doing so, we show a pre-assessment result of the service onboarding into EOSC Marketplace as most of the mandatory requirements are to be considered by each service provider during the evaluation of onboarding process.

The remaining sections of this document are structured as follows: section 2 gives a description of the service management framework and of the grouped requirements in different sections/groups.

Section 3 reports on the analysis we performed over seventeen services used as input during our evaluation.

Section 4 outlines recommendation for future integration work.

[1] https://www.fitsm.eu/
[2] https://www.coretrustseal.org/why-certification/requirements/
[3] https://doi.org/10.1038/s41597-020-0486-7
[4] https://doi.org/10.1038/s41597-020-0486-7
[5] https://doi.org/10.12688/f1000research.9656.2
[6] https://doi.org/10.1038/s41597-020-0486-7

Finally, Section 5 draws up the conclusions.

2 Service Management Framework

IT service management aims at providing high quality IT services meeting customers and users expectations by defining, establishing and maintaining service management processes [4].

A framework was adopted to define adequately these processes as needed.
This framework consists of 44 requirements and is divided into five sections:

- Service management (18 questions)
- Data repository requirements (14 questions) – section specific for data repositories only;
- Accessibility and legal requirements (5 questions)
- Sustainability (1 question)
- EOSC architecture compatibility (6 questions)

Every requirement is categorized either as *mandatory* or *optional*. Mandatory requirements (e.g., website, support contacts, documentation, privacy, and access policies, etc.) have to be achieved to publish that service in the EOSC portal. Optional ones are intended for going beyond the minimal level of service and provide actionable checks for the service managers.

In the following table we display an excerpt list with the requirements. For the full list you may read in detail the Annex 1.

Requirements		Source	Importance	Comment
1. Service management				
S-1	Web site where more information about the service can be found is publicly available	FitSM: Service Portfolio Management Process	mandatory	
S-2	Contact email address for end-users is publicly available	FitSM: Incident & Service Request Management Process; EOSC portal service requirements for providers	mandatory	
[..]	[..]	[..]	[..]	[..]
2. Data repository requirements				
D-1	Repository is certified	CTS (CoreTrustSeal)	mandatory	
D-2	Repository ensures that data deposited are released with a clear and accessible data usage license	CTS, COAR	mandatory	
[..]	[..]	[..]	[..]	[..]
3. Accessibility and legal requirements				
L-1	The service is accessible by users outside its original community	EOSC portal service requirements for providers	optional	For example, a user coming from social sciences is most likely non-native user in case he/she would like to use services provided by climate science community.
L-2	Service usage form other EU countries is possible		optional	
[..]	[..]	[..]	[..]	[..]
4. Sustainability				
F-1	Status in terms of service lifecycle is publicly available		mandatory	
5. EOSC architecture compatibility (to be included when documents and services become available)				
A-1	EOSC monitoring and reporting implemented	To be considered when description is available, recent documentation available here	optional	For monitoring only there is a guidance but not for reporting.
A-2	EOSC AAI implemented	To be considered when description is available, recent documentation available here	optional	
	[..]	[..]	[..]	[..]

Table 1. An excerpt list of requirements

Service case studies

To help SPs to manage their service(s), and thus provide value and customer service excellence in a simple way, we suggest this model as a go-to tool to be run by them. We received seventeen service assessments as feedback.

We suggest running this tool again in the future (on regular basis) to support the high-quality delivery of these services as potential candidates to EOSC.

The service types are as follows:

- **eight** cases are thematic services: Laniakea@ReCaS (INFN) - Italy; D4Science resource catalogue VRE (CNR) - Italy; Marketplace-pilot (Fraunhofer) – Germany; GPU container as a Service (CNRS) – France; VIP(CNRS)-France; AstroODA(ISDC/APC)-Switzerland; Simbad (CDS)-France and ReadMetrics(Inist-CNRS)-Luxembourg
- **five** cases are research data management services: B2SAFE provided by two national infrastructure providers: B2SAFE (KIT) - Germany; B2SAFE (CINES) - France and iRODS (FG) - France and as data repository service: datainrae (INRAE) – France and SWH(INRIA)-France
- **four** cases as generic(common) services: Cloud, HPC, VM and data storage: CLOUD (GARR) - Italy; HPC (CINECA) - Italy; as data archive: VITAM (CINES) - France and as computing resource: VM (KIT) - Germany

A list of these cases (services) endpoint and description is reported in **Errore. L'origine riferimento non è stata trovata.**Annex 2. All the cases are selected as potential EOSC service candidates.

3 Validation

In order to determine the status of the service offering, a subset of the existing SPs was selected to analyse their services from a service delivery perspective. We used a checklist template with requirements as a data collection tool. There were three options for answering a question: (*Yes*, *No*, and *N/A*) along with the additional explanation for the answer (as an evidence), specifically for questions answered as *Yes*.

We invited service managers/owners responsible for these seventeen services to respond to the maturity tool.

The service assessors had the possibility to clarify the requirements beforehand with the team through a dedicated meeting. Only one SP needed support for further clarification on the template and thus minimise potential misunderstandings. It shall be noted that the tool was also presented during one WP7 meeting in which most of the service managers were present.

The analysis covers seventeen services in total and is divided in different categories. Some of these services supply a more focused set of functionalities to their users and their communities. Other services supply a wide range of functionality and support a wide range of use cases in their communities.

We classified the services either as *ready-to-use* (part of WP7.4); *in-kind* services (resources available from existing partners as published in the grant agreement) and *new* services as thematic services selected from the open call launched in WP6. Three among the six selected applications agreed to provide their feedback on the checklist template. The service categories included in the analysis are either generic services such as VMs, cloud, HPC services, and data storage or thematic services such as Laniakea@ReCaS, resource catalogue through virtual research environment or data management such as data repository services.

Findings

After having all the results from the SPs, we have summarized in the following figure (with subfigures for the classified services) how each of them perform in the service delivery activity by providing a general score taking into account all requirements, and a specific score taking into account only mandatory requirements. The latter mostly corresponds to the current EOSC requirements proposed in order to onboard a service to the EOSC catalogue. During the lifetime of the project some of the service providers have successfully registered their resources/services into EOSC marketplace. These services are marked with an asterisk (*) before their service name. The validation statistics are reported in the following sections.

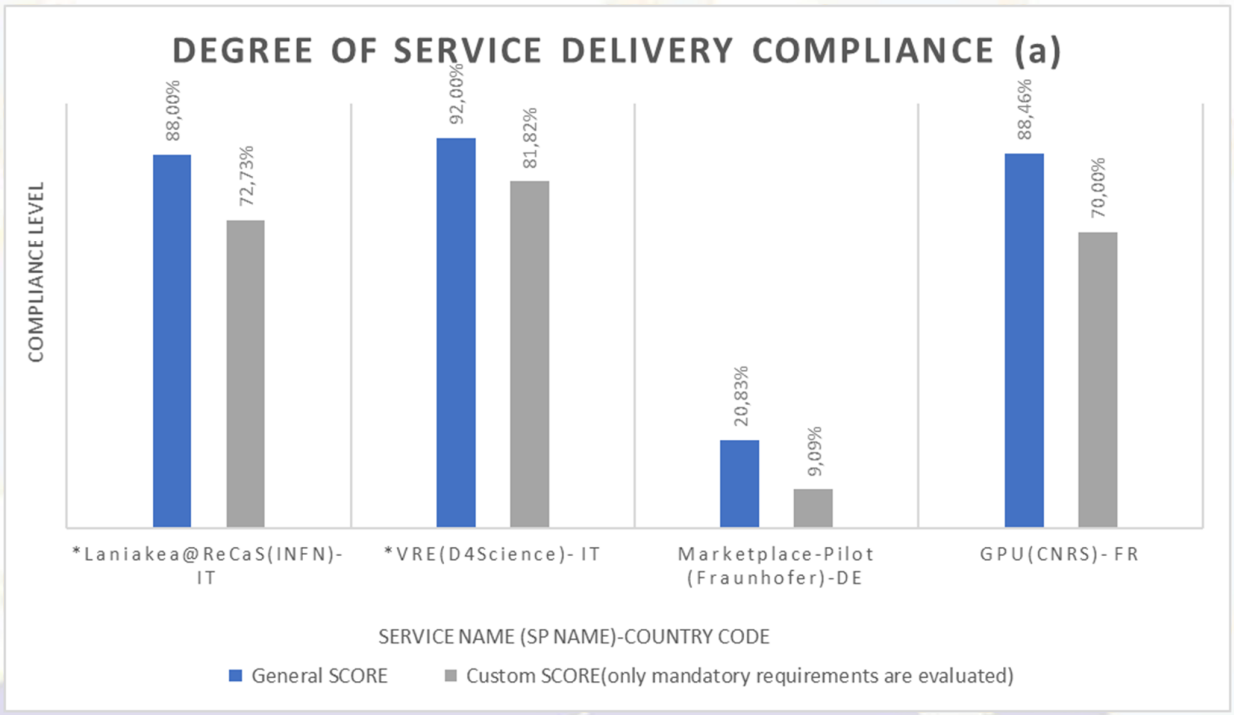

Fig. 1.a Service delivery compliance assessment (a)-*ready-to-use* services

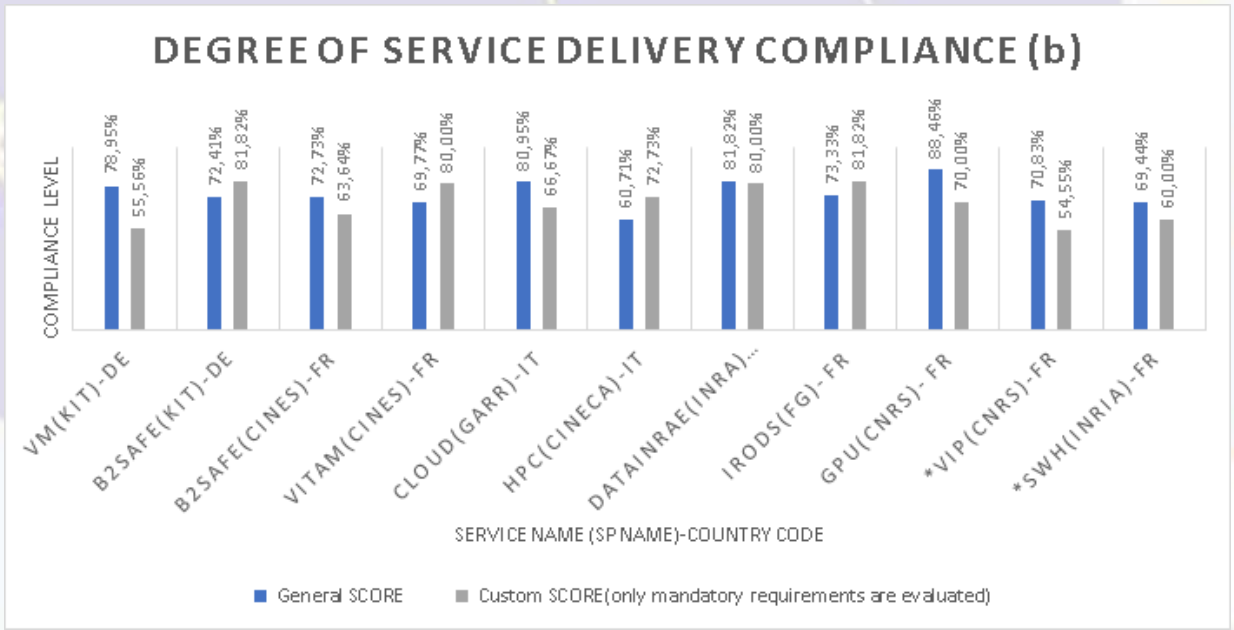

Fig. 2.b Service delivery compliance assessment (b)-*in-kind* services

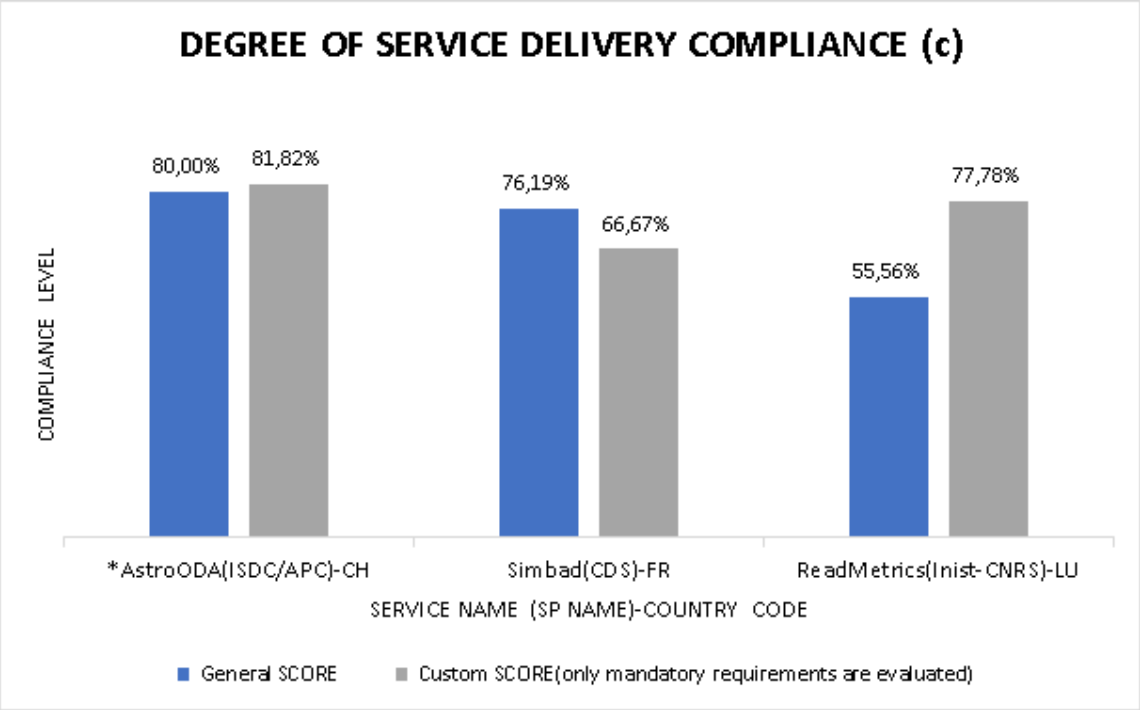

Fig. 3.c Service delivery compliance assessment (c)-*new* services

Fig. 4 Service delivery compliance assessment full overview

As seen from Fig. 1, each service reports a moderate or a high degree of compliance for service delivery using both of the scoring formulas except for the "Marketplace" service that is still labelled as a pilot and is still under development.

We report (commented in following subsections) as well how each of these services complies with the different defined requirements sections such as:

1. Service Management
2. Data repository requirements (only two services from our list)
3. Accessibility and Legal Requirements
4. Sustainability
5. EOSC architecture compatibility (to be included when documents and services become available)

The matrix shown in Fig. 2 presents the calculated degree of compliance based on the responses to our checklist template. The individual results for each service were calculated as a sum of all responses to all answers submitted in the requirements. For instance, the result of 83,33% for "Service management" for ***Laniakea@ReCaS*** was calculated as a sum of all Laniakea@ReCaS positive (i.e., 'yes') responses to the questions under the first section "1. Service management requirements" and then

divided this sum by the number of questions (18) covered in that section. We applied a conditional formatting rule (i.e., the icon sets: coloured arrow symbol) to each of the value cells to assess easily which is the compliance level for each service in relation to each requirements sections and their derived aggregations.

Category Requirem / Compliance Level	*Lanlaka@ReCaS	*VRE	Marketplace (pilot)	GPUaaS	Aggregate
1. Service management	83,33%	94,44%	27,78%	83,33%	72,22%
3. Accessibility and legal requirements	100,00%	80,00%	0,00%	60,00%	60,00%
4. Sustainability	100,00%	100,00%	0,00%	100,00%	75,00%
5. EOSC architecture compatibility	25,00%	25,00%	0,00%	100,00%	37,50%
Aggregate	77,08%	74,86%	6,94%	85,83%	61,18%

High compliance [>67%]
Medium compliance [>=33% and <67%]
Low compliance [<33%]

Fig. 2.a A submatrix displaying the calculated degree of the service delivery compliance for *ready-to-use* service in relation with the requirements category

Category Requirements / Compliance Level	VM	B2SAFE(KIT)	B2SAFE(CINES)	VITAM	CLOUD	HPC	DataImage	iRODS	*VIP	*SWH	Aggregate
1. Service management	61,11%	83,33%	66,67%	61,11%	66,67%	72,22%	83,33%	88,89%	61,11%	66,67%	71,11%
3. Accessibility and legal requirements	60,00%	80,00%	80,00%	100,00%	80,00%	60,00%	80,00%	100,00%	100,00%	80,00%	82,00%
4. Sustainability	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5. EOSC architecture compatibility	0,00%	25,00%	0,00%	20,00%	0,00%	0,00%	50,00%	0,00%	0,00%	33,33%	12,83%
Aggregate	55,28%	72,08%	61,67%	70,28%	61,67%	58,06%	78,33%	72,22%	65,28%	70,00%	66,49%

High compliance [>67%]
Medium compliance [>=33% and <67%]
Low compliance [<33%]

Fig. 2.b A submatrix displaying the calculated degree of the service delivery compliance for *in-kind* service in relation with the requirements category

Category Requiremen Compliance Level	High compliance [>67%] / Medium compliance [>=33% and <67%] / Low compliance [<33%]	*AstroO DA	Simbad	ReadMetrics	Aggregate
1. Service management		100,00%	61,11%	61,11%	74,07%
3. Accessibility and legal requirements		80,00%	80,00%	60,00%	73,33%
4. Sustainability		100,00%	100,00%	100,00%	100,00%
5. EOSC architecture compatibility		16,67%	0,00%	0,00%	5,56%
Aggregate		74,17%	60,28%	55,28%	63,24%

Fig. 2.c A submatrix displaying the calculated degree of the service delivery compliance for *new* service in relation with the requirements category

Fig. 2 A matrix displaying the calculated degree of the service delivery compliance for each service in relation with the requirements category

We derive a graphical illustration of the above aggregation metrics as displayed in the following plot of Fig. 3.

As seen from the plot (Fig. 2.a) the service with the highest average level is ***GPUaaS*** from the first category group as ready-to-use whereas the service with the lowest value is the ***Marketplace***. Whereas from plot in Fig.2.b in the category of in-kind service, the service with the highest and lowest values are respectively ***DataInrae*** and ***VM***. And last from plot in Fig.2.c in the category of the new thematic services the highest and lowest value are respectively ***AstroODA*** and ***ReadMetrics***.

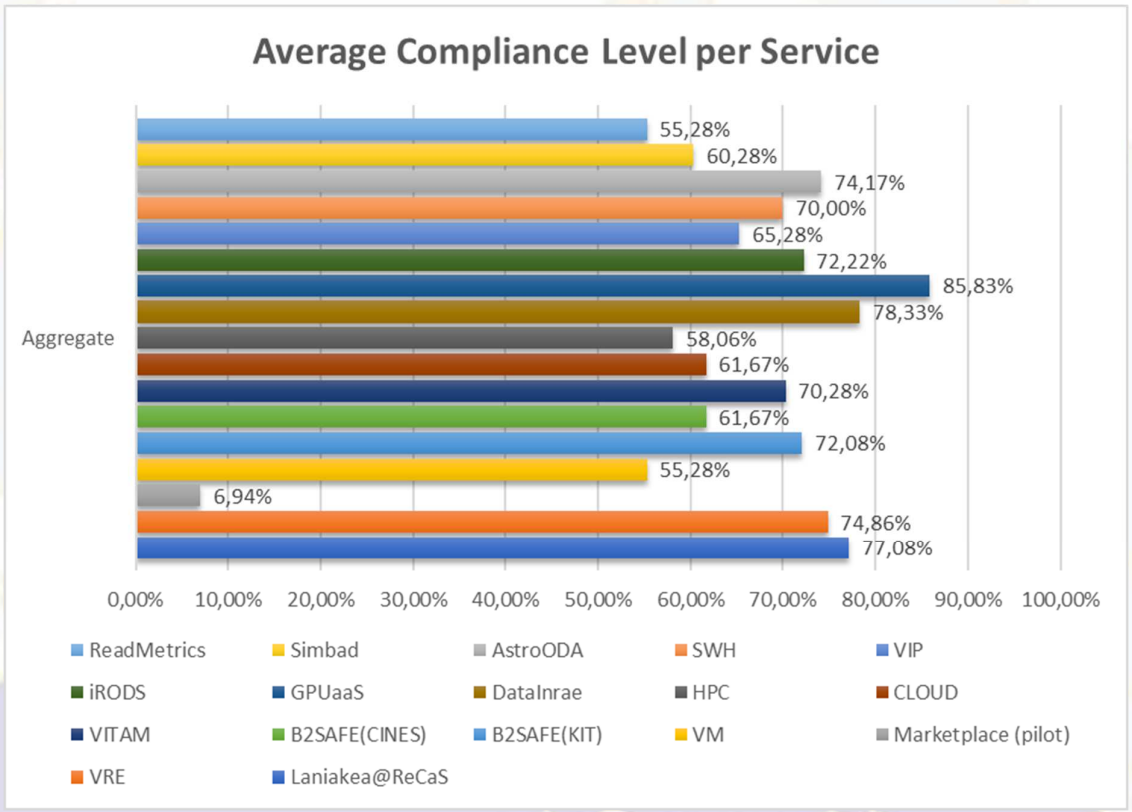

Fig. 3 The average calculated degree of compliance for each service

Instead, in Fig. 4 we report on the average compliance level of service per each category requirements. The second category named “2. Data repository requirements” is not displayed as this is typical for those data managers that are offering data repository as a service. We report on these values on Section 3.1.2.

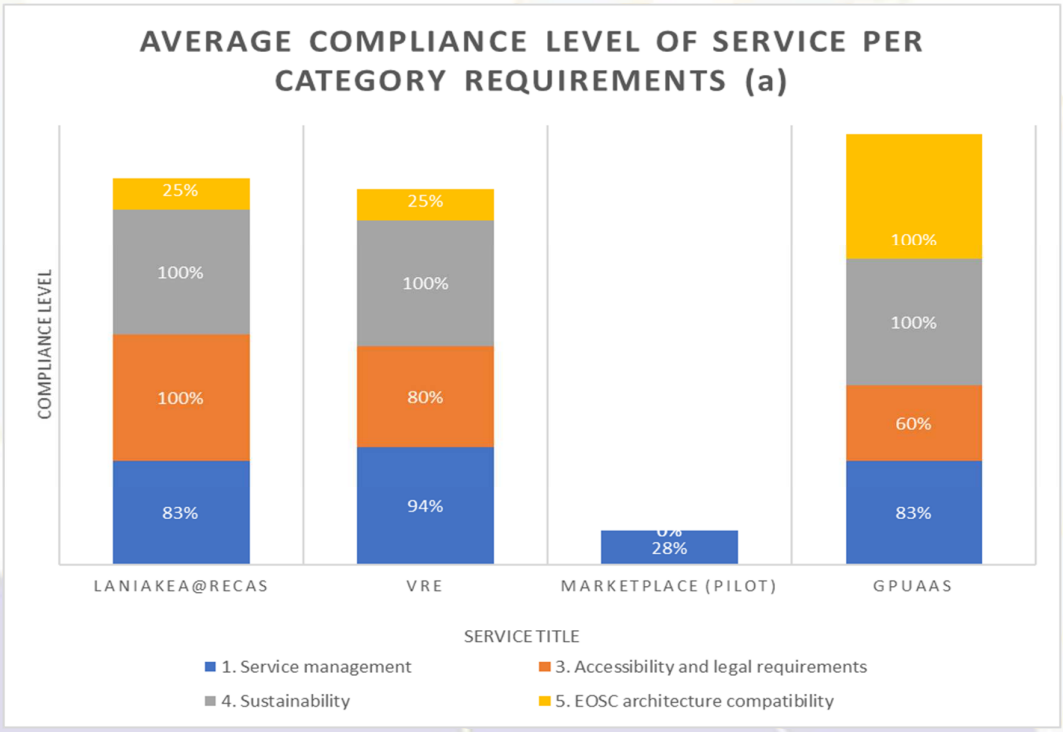

Fig. 4.a The average calculated degree of compliance of *ready-to-use* service per requirements category

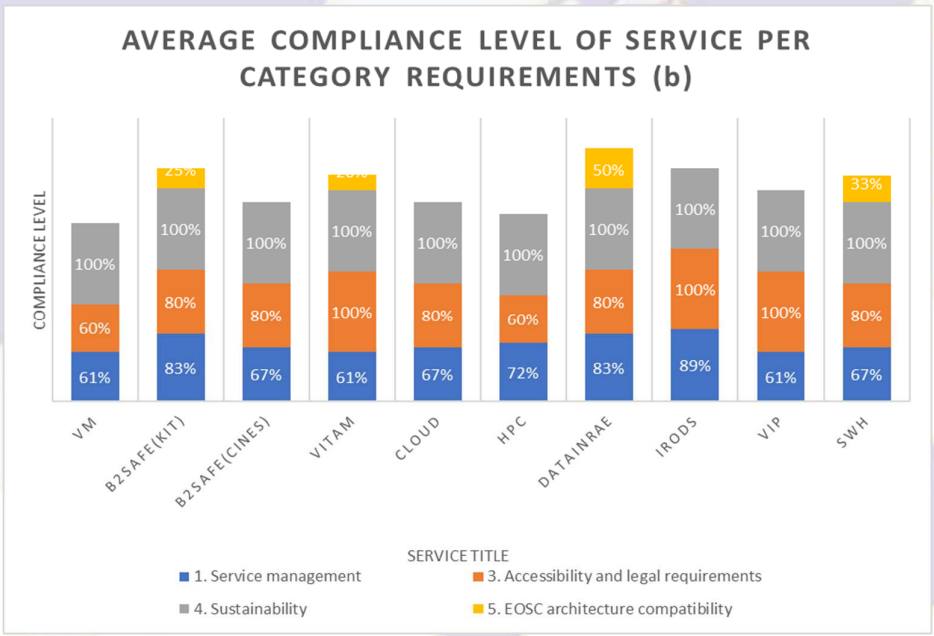

Fig. 4.b The average calculated degree of compliance of *in-kind* service per requirements category

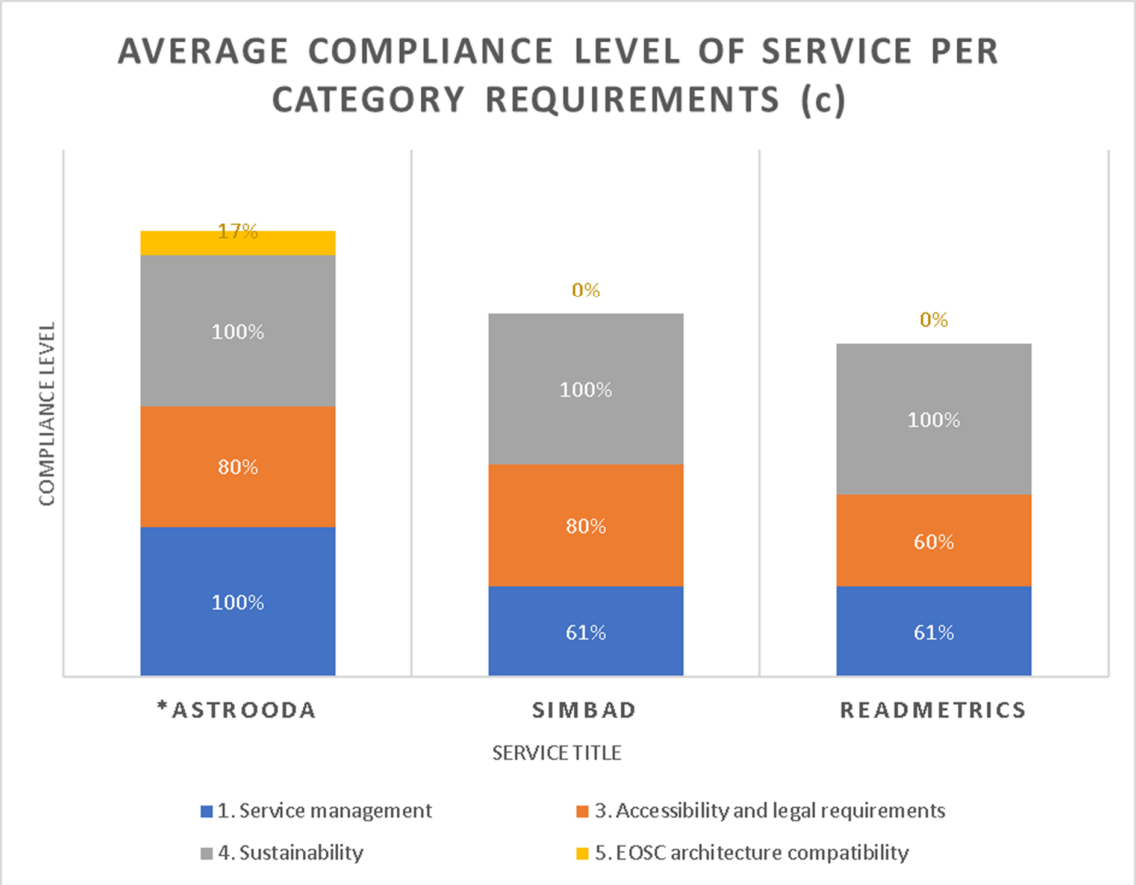

Fig. 4.c The average calculated degree of compliance of *new* service per requirements category

Fig. 4 The average calculated degree of compliance of each service per requirements category

As seen from the above clustered columns graph, all services demonstrate a moderate or a high degree of compliance for service delivery in all the category requirements except for the last one named "5. EOSC architecture compatibility". Thorough analysis shows that the SP implemented and deployed their own solution for monitoring, accounting, reporting and although many of them have already complied with the requirement "A-2: EOSC AAI implemented", yet they still need to comply with "A-5: EOSC Data Transfer Services implemented" and "A-6: Persistent identifier with required metadata for services".

3.1.1 Service Management

This section contains the highest number of requirements (i.e. 18). Eight services achieved more than 72% degree of compliance, eight a moderate degree and one a low degree. The service with the low compliance was due to the status of the service as being in pilot. All the mandatory requirements in this section such as web service address, contact address or service documentation are almost fully met by all the

services, while requirements such as disaster recovery issues and service level target result in a moderate compliance. Either some of the services did not meet this requirement as defined to be publicly available or they commented that they have considered it but the respective documentation is not for public use as its access is restricted.

3.1.2 Data repository requirements

The two services that fall in the category of data repository services achieved a very high degree of compliance with all the requirements in this section as shown in Fig. 5.

All of them did not meet the first requirement "D-1: Repository is certified", by giving two arguments: one is that they are in the process of applying to CTS and the other commented that their previous version of long-term preservation data repository was DSA (Digital Seal of Approval) certified.

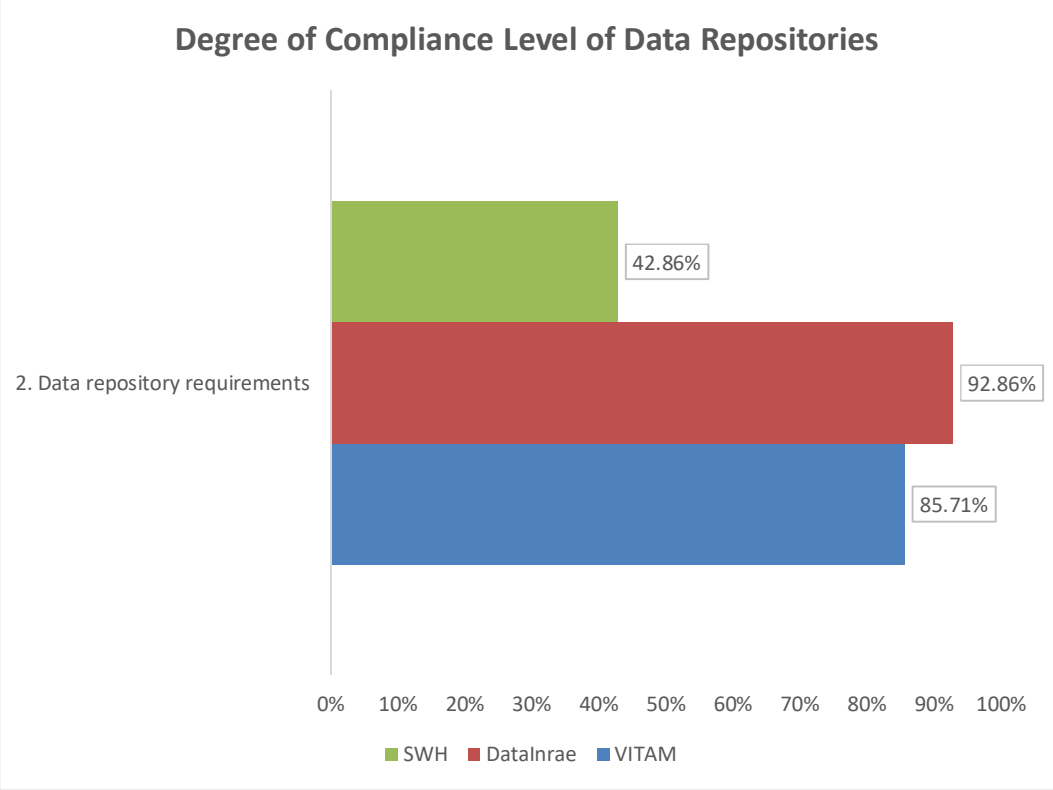

Fig. 5 The calculated degree of compliance for two data repository services

3.1.3 Accessibility and Legal Requirements

The services achieved a high degree of compliance with these requirements (i.e. 14). This is reflected in compliance with Service usage outside its original community and from other EU countries, GDPR is clarified, while requirement dealing with liabilities of contracts and subcontracts that has to be limited results in almost fully compliance.

3.1.4 Sustainability

The services achieved almost 100% compliance on the requirement defined in this section, about making publicly available the service status in terms of service life cycle, e.g., pilot, production or discontinued.

3.1.5 EOSC architecture compatibility

The services achieved a low degree of compliance, 17,35% on average (see Fig. 6). The lowest compliance is in relation to questions regarding the monitoring, accounting, and reporting, while for questions related to the AAI some of them have already complied with it.

This low-level degree of compliance is somewhat justified as only recently the corresponding documentation and guidelines have been published as we explained in the last paragraph of Section 0

Relation to EOSC Portfolio enhancement

The model maturity tool we complemented may contribute towards enhancing the EOSC portfolio with these new potential services. Therefore, this work helped to guide the SPs and to support them to deliver services that will meet the user expectations and satisfy them. It also complements the work they should consider in order to get a positive evaluation during the onboarding process in EOSC catalogue and Marketplace.

4 Recommendation for future integration work

One of the wonderful effects of open science and the work on EOSC is that communities are looking to integrate their IT services and developments with the large infrastructures, not only in their home country but as well into the EOSC environment. This is proven by the work done in WP7 of EOSC-Pillar and described in this deliverable. Not only does this improve visibility of the research done to develop and implement the services, it also contributes to all aspects of Open Science and the FAIR paradigm. In effect a service as part of the EOSC ecosystem can be found via the EOSC catalogue and is accessible using the federated AAI. Furthermore the service promotes interoperability as well as re-use the moment researchers from outside the organisation that delivers the service, employ the offering in their own research.

At the same time, and this is an important lesson learned in Task 7.2 and 7.3, interoperation of services is most successful when providers have a good understanding of requirements on both sides and they benefit from short communication lines during the time of integration. This does not mean that documentation or experience is lacking, though improvement is always possible, rather the detailed (in)dependencies lead to unexpected hurdles that can only be overcome after intricate deliberation and attention to detail from both sides.

Based on the lessons learned and on the produced statistics we list the recommendations in different types as follows:

Organisational Dependencies

As the work progressed, it quickly became clear that a service is not a stand-alone entity and is in most cases dependent on additional services. Apart from its AAI federation or the nomination in a services catalogue, e.g the EOSC catalogue[7], a service will depend on third party or underpinning services. E.g a repository relies on a storage or compute resource that is offered by an external provider. Or, a work-flow engine that depends on the access of published data that is referenced via a PID provided by a PID service. The depth and complexity of this network consisting of interwoven connections between service building blocks offered by different or even transnational providers will certainly increase while EOSC develops.

- An increasing number of interdependencies between underpinning services pose a risk to the overall reliability of a top level service

  For this aspect, sustainability is also a factor. Service implementers and researchers alike, prefer to rely on a solid provider and service offering as they are not keen in shifting to another provider in the short term because of the

[7] https://eosc-portal.eu/

learning curve for using a news services and the associated work needed to adapt their set-up. Assessing and valuing the future reliability and resilience of a service provider is therefore equally important as all other factors determining the choice for a service. This will become even more important over time when automated selection and pairing of services replace direct contacts between implementers and providers that have been beneficial in the work in this task. The assurance of the sustainability of a prospective service is evenly important for an implementer as for a researcher.

Also the dependencies have to be well understood to be able to update the top level interfaces when necessary. The communication channels must be well organised to disseminate the need of updates.

- an indication of reliability and sustainability of a service offering should be transparent and ensured impartially to support correct selection of the service by potential end-users i.e. researchers, as well as by implementers of a new service that makes use of the service.

As more services will become dependant on underpinning services the, e.g cloud storage or cloud computing, these components should be clear to the potential customer. We realise this openness is not always possible or wanted. This recommendation implies also that a recurring evaluation of the service must include a re validation of the reliability and the sustainability.

Technical Dependencies

- Existing software should stay aligned with developments in related software. Conventional software and tools exists that, despite their continuous improvement, do not comply with some of the newer developments related to federated access. For instance, federated access in iRODS, is not part of the main development branch. A modern protocol like OIDC (Open ID Connect) that implements the identity layer to allow clients to confirm an end-user identity using authentication by an authorization server, is not available for the iRODS backend. Practically, this example leads to recommend the adoption of modern protocols specifically for software already developed and being used since a long time. Gaps defined as a feature/function missing from a service and that does not meet user expectations should be identified and narrowed/closed. For example to represent geographical data from data portals the GeoDCAT-AP[8] profile should be embedded as an extension of the metadata repository (called Federated FAIR data space=F2DS) developed in the project framework. This extension is going to be configured in the second release of the F2DS software to meet the requirement of one of the use cases in WP6. This gap will be closed by the service provider.

[8] https://inspire.ec.europa.eu/good-practice/geodcat-ap

- Service delivery shall be improved in relation to the mandatory requirements for those services that lacks in this regard or that do not fully support them.
- After a service reaches the highest degree of compliance shift the focus to improve the delivery across other countries in Europe by making available SLAs and relevant documentations in English language if not exist already.
- Most of the requirements categorized in “5. EOSC architecture compatibility”, were not considered bysome of SPs because either the SP implemented and deployed their own solution for monitoring, accounting, reporting or the information on how to achieve the technical integration was missing (e.g. “A-5: EOSC Data Transfer Services implemented” and “A-6: Persistent identifier with required metadata for services”) or not available by that time.

Dissemination of Information

- Disseminate the information about the concrete list of the available federation services and in general all the EOSC core services, and their technical integration guidelines to effectively reach and involve the target audiences (providers, services developers).

5 Conclusions

In this report we described the readiness of the services to be used by external users, specifically users coming from a European country different from the one of original users.

To do this assessment we used the maturity model assessment tool proposed by WP3 of the EOSC Nordic project which we further updated to match our scope and use case. We have been in contact with EOSC Nordic WP3 team to exchange information on the different versions released of the maturity tool.

Our analysis indicates that the services achieve an overall medium (64.67%) level compliance to the service delivery requirements. Hence, they already comply with most of the EOSC onboarding validation criteria and are ready to serve a broader range of users.

After executing the analysis, we reflected on possible improvements or further work, for example to involve existing end-users to evaluate these requirements, and/or improvement of existing requirements, and/or examine the rest of the services in our project or regularly run this tool to see if improvements are made by the SPs.

References

[1]. https://www.eosc-nordic.eu/content/uploads/2020/06/Maturity-model-checklist-template-ver2.xlsx
[2]. https://docs.google.com/spreadsheets/d/1zeUShdnFQU5fTeKSyOcvlCCKeGMA6sbnp7bUkXaa97k/edit#gid=1115091576
[3]. https://docs.google.com/spreadsheets/d/19bptRYOBdlsEg6Hwv7m2gO1Z1EHJPeLYan1AuRRUmNA/edit#gid=0
[4]. https://www.fitsm.eu

Annex 1 Checklist template

The actual file used to collect feedback is available from the EOSC-Pillar repository: https://repository.eosc-pillar.eu/index.php/s/JqHSqgowzPT7yEa

Such file contains the following template, as well as the spreadsheet used to compile scores for each service.

Requirements		**Source**	**Importance**	**Comment**
1. Service management				
S-1	Web site where more information about the service can be found is publicly available	FitSM: Service Portfolio Management Process	mandatory	
S-2	Contact email address for end-users is publicly available	FitSM: Incident & Service Request Management Process; EOSC portal service requirements for providers	mandatory	
S-3	Contact address for security issues is publicly available	FitSM: Incident & Service Request Management Process	mandatory	
S-4	Service documentation for end users is publicly available	FitSM: Service Portfolio Management Process, EOSC portal service requirements for providers	mandatory	
S-5	Disaster recovery possibilities for research data are publicly described	FitSM: Incident & Service Request Management Process	optional	It is enough to say what are the possibilities to recover data.
S-6	Detailed service installation documentation exist.		optional	Service can be reimplemented in reasonable time should it be necessary
S-7	Automatic software upgrades have been implemented or there is an alternative policy/practice enabling rapid responses to software vulnerabilities	FitSM: Information Security Management	optional	There is some kind of automatic software patching method implemented or there is a guideline/policy describing who software vulnerabilities are recognized, analyzed and reacted.

S-8	Service availability is monitored and availability information is publicly available and service users should be notified	FitSM: Service Level Management, FitSM: Service Availability & Continuity Management	mandatory	It is enough to have measured availability number in public web page. E.g. availability during last month or something similar
S-9	Service level target is defined and it is publicly available	FitSM: Service Level Management	mandatory	SLT refers to the expected delivery time of the service. SLT is about expected performance(e.g. 90% target) and comprise: deliverySLT, responseSLT, resolutionSLT, based on three values: target days/h/min
S-10	Service capacity is monitored	FitSM: Capacity Management	optional	Capacity here is e.g. data volume, data transfer bandwidth, number of standard analysis /hour, …
S-11	Service capacity limits are known	FitSM: Capacity Management	mandatory	Service capacity is explicitly known (i.e. volume of data) or maximum capacity is estimated/tested in reasonably reliable way
S-12	Service usage metric is defined and followed		optional	There is a metric that can be used to define how much the service is used. This metric is followed and it can be reported to e.g. project funders.
S-13	Information about maintenance breaks is publicly available and service users should be notified	FitSM: Service Level Management	mandatory	
S-14	There is a document, that is used to ensure that the service behaves normally after implemented changes	FitSM: Release & Deployment Management	optional	This could be e.g. a set of verification tests with expected results and expected run times, etc.
S-15	Service release notes or similar documentation describing changes in service is publicly available	FitSM: Service Portfolio Management Process, EOSC portal service requirements for providers	optional	It is enough to have information that can be considered to be relevant to service end users.
S-16	Channel to recommend service enhancements exists	FitSM: Continual Service Improvement Management	optional	
S-17	Service roadmap exist and it is public		optional	At some level, information about service future is public. Roadmap could e.g. describe versions of software components in next service releases.
S-18	A report of ensuring service production according to specifications in a timely manner to support decision-making	FitSM:Service reporting management	optional	
2. Data repository requirements				

D-1	Repository is certified	CTS (CoreTrustSeal)	mandatory	
D-2	Repository ensures that data deposited are released with a clear and accessible data usage license	CTS, COAR	mandatory	
D-3	Repository supports harvesting of metadata using OAI-PMH	COAR	mandatory	OAI-PMH is a standard metadata harvesting protocol
D-4	Repository ensures ongoing access to resources for a publicly stated time	COAR	mandatory	
D-5	In cases where there is restricted access to a resource, the repository facilitates an indirect way to access this resource (e.g. by contacting the author)	COAR	optional	
D-6	Repository supports quality metadata and controlled vocabularies (discipline-based, regional or general metadata schema such as Dublin Core)	COAR,NIH	mandatory	Metadata: Ensures datasets are accompanied by metadata to enable discovery, reuse, and citation of datasets, using schema that are appropriate to, and ideally widely used across, the community(ies) the repository serves.
D-7	The metadata in the repositories are available in human-readable and machine-readable formats	COAR	optional	
D-8	The resources are stored in machine-readable, community standard formats	COAR	optional	
D-9	Repository supports PIDs for resources(data)	COAR,NIH	mandatory	E.g. a DOI=digital object identifier; ensures proper citation, discovery, reporting
D-10	Repository supports PIDs for authors, funders, funding programmes and grants, institutions, and other relevant entities	COAR	optional	
D-11	Repository provides documentation or has a policy that outlines the scope of content accepted into the repository	COAR	mandatory	describe the scientific coverage and comprehensiveness of the resource.
D-12	The metadata in the repository are available, even in cases when the resource is no longer available	COAR	mandatory	Longterm sustainability support
D-13	Repository is included in one or more disciplinary or general registries of resources	COAR	optional	e.g. in re3data.org as a registry of research data repositories

D-14	Repository clearly indicates what organization is responsible for managing it	COAR	mandatory	
3. Accessibility and legal requirements				
L-1	The service is accessible by users outside its original community	EOSC portal service requirements for providers	optional	For example, a user coming from social sciences is most likely non-native user in case he/she would like to use services provided by climate science community.
L-2	Service usage form other EU countries is possible		optional	
L-3	Terms Of Use is available		mandatory	
L-4	Limitation of liability in contracts and contract chains: * Damages has to be limited		optional	Service provider can only sell those rights that a service provider has. Service provider is responsible of subcontractors work and possible damages caused by subcontractors. Considering possible risks, following two scenarios can be considered: Low risk scenario No subcontractors are used and only free and non-restrictive service components are used. Possible limitations of liabilities can be defined e.g. in "Terms of Use" document. Other cases Service provider has to check what rights it has to service components. Limitations of liability (contractual penalties, damages, force majeure clauses, warrenties) between a service provider and possible subcontractors (and chain of subcontractors) has to be checked.
L-5	GDPR * GDPR status of a service has been clarified * If the service contains or processes personal data, GDPR implications have been identified * If the service contains or processes personal data, service fulfils GDPR requirements	GDPR	mandatory	Personal data is defined e.g. here: https://tietosuoja.fi/en/what-is-personal-data Logged IP addresses are examples of personal data.
4. Sustainability				
F-1	Status in terms of service lifecycle is publicly available		mandatory	
5. EOSC architecture compatibility (to be included when documents and services become available)				

A-1	EOSC monitoring and reporting implemented	To be considered when description is available, recent documentation (from EOSC-Hub project) available here	optional	For monitoring only there is a guidance but not for reporting.
A-2	EOSC AAI implemented	To be considered when description is available, recent documentation (from EOSC-Hub project) available here	optional	Documentation provided by T7.1 to guide the SPs to integrate their service with Indigo-IAM Pillar instance as one of the EOSC AAI solution
A-3	EOSC monitoring implemented	To be taken into account when description is available, recent documentation (from EOSC-Hub project) available here	optional	
A-4	EOSC accounting implemented	To be taken into account when description is available, recent documentation (from EOSC-Hub project) available here.	optional	
A-5	EOSC Data Transfer Services implemented	To be taken into account when description is available	N/A	
A-6	Persistent identifier with required metadata for services	To be taken into account when description is available	N/A	

Table 1. Checklist requirements template

Annex 2 List of services descriptions used as case studies

Ready-to-use services					
Provided Service (ready-to-use)	**Provider**	**Generic name/ Service Endpoint**	**Service description**	**Authentication**	**Request from**
***Laniakea@ReCaS(INFN)-IT**	INFN	Laniakea@ReCaS -Galaxy as a Service/ https://laniakea-dashboard.cloud.ba.infn.it	Laniakea (https://laniakea-elixir-it.github.io) is a software framework that facilitates the provisioning of on-demand Galaxy instances as a cloud service over e-infrastructures.	INDIGO-IAM	UC6
***VRE(D4Science)- IT**	CNR-ISTI	D4SCIENCE/ https://eosc-pillar.d4science.org/group/eoscpillarresdatactlg	Every VRE/VLab realises a web-based working environment for a community to collaborate. It offers some basic and community agnostic services (e.g. workspace, social networking, user management) that can be complemented by community specific services to be integrated.	EOSC federation, Google, LinkedIn	UC3, T4.4, T5.4
Marketplace-Pilot (Fraunhofer)-DE	Fraunhofer-IWM	Materials Modelling Marketplace	Marketplace is a platform for collaboration and online materials modelling laboratories	Oauth2	UC3

GPU(CNRS)- FR	CNRS	GPU as a service/ https://sbghorizon.in2p3.fr/dashboard/auth/login/?next=/dashboard/	A container-based service has been recently added to meet user's needs and to face new challenges of scientific research. It permits to instantiate Kubernetes clusters, with the possibility to use GPUs. This service is currently only available on the Cloud infrastructure hosted by the SCIGNE platform.	EGI Checkin	UC3, UC5
in-kind services					
Provided Service (ready-to-use)	**Provider**	**Generic name/ Service Endpoint**	**Service description**	**Authentication**	**Request from**
VM(KIT)-DE	KIT	VIrtual Machine/ https://www.scc.kit.edu/dienste/9592.php	VMWare ESX is only for KIT internal.	local	
CLOUD(GARR)-IT	GARR	Cloud Compute/ https://cloud.garr.it/	The GARR Cloud Platform offers cloud services to the Italian academic and research community. GARR coordinates a federation of clouds, located in national datacenters owned by members of the GARR community, which participate to the federation by sharing resources and services.	local	

B2SAFE(KIT)-DE	KIT	B2SAFE/ https://eudat.eu/services/b2safe	B2SAFE is a robust and highly available service which allows community and departmental repositories to implement data management policies on their research data across multiple administrative domains in a trustworthy manner. It offers an abstraction layer of large scale, heterogeneous data storages, guards against data loss in long-term archiving, allows to optimize access for users (e.g. from different regions), brings data closer to facilities for compute-intensive analysis.	B2ACCESS	UC7
B2SAFE(CINES)-FR	CINES	B2SAFE https://eudat.eu/services/b2safe	B2SAFE is a robust and highly available service which allows community and departmental repositories to implement data management policies on their research data across multiple administrative domains in a trustworthy manner.	B2ACCESS	
VITAM(CINES)-FR	CINES	VITAM/ https://facile.cines.fr/	Vitam is an open source software able to manage and preserve digital records and archives	local	UC4
HPC(CINECA)-IT	CINECA	HPC/ https://www.hpc.cineca.it/services	CINECA provides a wide range of computing resources, being the Italian point of reference for High Performance Computing. For the main mission, supporting researchers from academia and industries in their computing-based research, we have continuously offered the leading-edge resources available,	local	UC2

			combined with advanced skills and expertise of the technical and scientific staff.		
DataInrae(INRA)-FR	INRAE	Data repository/ https://datapartage.inrae.fr/Partager-Publier/Deposer-dans-Data-INRAE	The INRAE Data portal offers new services to facilitate the management, sharing and research of Institute data.	local	UC3
iRODS(FG)- FR	CNRS	FG-iRODS	Is a data management service called FG-iRODS. It is based on the iRODS software.	local (INDICO-IAM)	UC2,UC3
***VIP(CNRS)-FR**	CNRS	Virtual Imaging Platform/ https://www.creatis.insa-lyon.fr/vip/ https://providers.eosc-portal.eu/service/creatis.virtual_imaging_platform	The Virtual Imaging Platform (VIP) is a web portal for medical simulation and image data analysis. It leverages resources available in the biomed Virtual Organisation of the EGI e-Infrastructure to offer an open service to academic researchers worldwide.	Local, SAML, EGI Checkin	COVID-19 use case
***SWH(INRIA)-FR**	INRIA	Software Heritage Archive/ https://www.softwareheritage.org	SWH is a universal software archive that collects and preserves software in source code form, because software embodies our technical and scientific knowledge and humanity cannot afford the risk of losing it.	INDICO-IAM	UC5
new thematic services from open call					

***AstroODA(ISDC/APC)-CH**	ISDC	Astrophysical Online Data Analysis https://www.astro.unige.ch/mmoda/	Is a web-based astrophysical analysis. An extensible open-source software framework for building and exchanging web-based astrophysical data analysis services, leveraged by international community	github logins (INDICO-IAM)	
Simbad(CDS)-FR	CDS	SIMBAD Astronomical Database / http://simbad.u-strasbg.fr/simbad/	The SIMBAD astronomical database provides basic data, cross-identifications, bibliography and measurements for astronomical objects outside the solar system. SIMBAD can be queried by object name, coordinates and various criteria	(INDICO-IAM)	
ReadMetrics(Inist-CNRS)-LU	INIST-CNRS	ReadMetrics https://readmetrics.org/	ReadMETRICS is a new turnkey solution for: monitoring transformative agreements, including before and beyond; analysing usage across disciplines and consortia; assessing value of publishing spend; enabling comparative citation analysis.	Identity Federation (subset of eduGAIN) (INDICO-IAM)	

Table 1. A list of service/resource descriptions

High compliance [>67%]
Medium compliance [>=33% and <67%]
Low compliance [<33%]

Category Requirements/ Compliance Level	Lantiaka@ReCaS	*VRE	MarketPlace (pilot)	VM	B2SAFE(KIT)	B2SAFE(CINES)	VITAM	CLOUD	HPC	DataInrae	GPUaaS	iRODS	*VIP	*SWH	*AstroODA	Sm bad	ReadMetrics	Aggregate
1. Service management	83,33%	94,44%	27,78%	61,11%	83,33%	66,67%	61,11%	66,67%	72,22%	83,33%	83,33%	88,89%	61,11%	66,67%	100,00%	61,11%	61,11%	71,90%
3. Accessibility and legal requirements	100,00%	80,00%	0,00%	60,00%	80,00%	80,00%	100,00%	80,00%	60,00%	80,00%	60,00%	100,00%	100,00%	80,00%	80,00%	80,00%	60,00%	75,29%
4. Sustainability	100,00%	100,00%	0,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	94,12%
5. EOSC architecture compatibility	25,00%	25,00%	0,00%	0,00%	25,00%	0,00%	20,00%	0,00%	0,00%	50,00%	100,00%	0,00%	0,00%	33,33%	16,67%	0,00%	0,00%	17,35%
Aggregate	77,08%	74,86%	6,94%	55,28%	72,08%	61,67%	70,28%	61,67%	58,06%	78,33%	85,83%	72,22%	65,28%	70,00%	74,17%	60,28%	55,28%	64,67%

Fig. 6 A matrix displaying the calculated degree of the service delivery compliance for each service in relation with the requirements category