

D3.3 Service Interoperability Framework

Author(s)	Ari Lukkarinen (CSC), Dejan Vitlacil (SNIC), Morten Kjeldgaard (DeIC), Leah Riungu-Kalliosaari (CSC)
Status	Submitted
Version	1.0
Date	11/11/2020

Document identifier:	
Deliverable lead	CSC
Related work package	WP3
Author(s)	Ari Lukkarinen (CSC), Dejan Vitlacil (SNIC), Morten Kjeldgaard (DeIC), Leah Riungu-Kalliosaari (CSC)
Contributor(s)	Anders Sjöström (SNIC), Troels Rasmussen (DeIC), Ilja Livenson (ETAIS/UT), Ahti Saar (ETAIS/UT), Lauris Cikovskis (RTU)
Due date	31/10/2020
Actual submission date	11/11/2020
Reviewed by	Andreas Jaunsen (Nordforsk), Kessy Abarenkov (ETAIS/UT)
Approved by	
Dissemination level	Public
Website	https://www.eosc-nordic.eu/
Call	H2020-INFRAEOSC-2018-3
Project Number	857652

Start date of Project	01/09/2019
Duration	36 months
License	Creative Commons CC-BY 4.0
Keywords	Service(s), interoperability, framework(s)

Abstract:

This document aims at enhancing interoperability of the Nordic and Baltic services that are relevant for EOSC. It looks at the recommendations provided in the European Interoperability Framework and the EOSC Interoperability Framework (currently as a draft) and considers their suitability and applicability within the scope of Nordic and Baltic services. The deliverable provides observations about service interoperability across different services.



Copyright notice: This work is licensed under the Creative Commons CC-BY 4.0 licence. To view a copy of this licence, visit <https://creativecommons.org/licenses/by/4.0>.

Disclaimer: The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the document is believed to be accurate, the author(s) or any other participant in the EOSC-Nordic Consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the EOSC-Nordic Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the EOSC-Nordic Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Table of Contents

1. Introduction	4
1.1 Objectives and context	4
1.2 Definitions	4
1.3 How to read this deliverable	5
2. Interoperability Frameworks	5
2.1 European Interoperability Framework	5
2.2 EOSC Interoperability Framework	6
3. Selected recommendations	7
3.1 Methodology	7
3.2 Recommendations, questions and the reasoning for their selection	7
3.2.1 Core interoperability principles	7
3.2.2 Generic user needs and expectations	9
3.2.3 Legal interoperability	9
3.2.4 Technical and organisational interoperability	10
3.2.5 Semantic interoperability	11
3.2.6 Conceptual model	11
3.3 Service case studies	12
4. Analysis	13
4.1 Findings	13
4.1.1 Core interoperability principles	14
4.1.2 Generic user needs and expectations	15
4.1.3 Legal interoperability	15
4.1.4 Technical and organisational interoperability	15
4.1.5 Semantic interoperability	15
4.1.6 Conceptual model	15
4.2 Reflections on responses from service providers	15
4.2.1 Should end-user behavior be in scope?	15
4.2.2 Do one-size-fits-all questions apply?	16
4.2.3 Will future user requirements increase the importance of interoperability frameworks?	16
4.3 Recommended further work	16
4.4 Relation to EOSC development	17
4.5 Summary	18
5. Conclusions	18

I. Introduction

This document is produced as part of ongoing efforts within WP3 of the EOSC-Nordic project. The task specifically aims at fostering service interoperability in the Nordics and Baltics; and proposing suggestions for improving the interoperability approach within EOSC.

The EOSC interoperability approach has, so far, focused mainly on data and research outputs. An efficient research data lifecycle is supported by services, software and infrastructure. Therefore, it is very important to focus not only on research outputs, but also on the underlying enabling aspects and mechanisms. With that in mind, our work aims at highlighting service interoperability aspects relevant for all services geared towards open science.

I.1 Objectives and context

The work presented in this deliverable aims at contributing towards ongoing discussions on interoperability frameworks, specifically with services in mind. We leverage on existing interoperability guidelines, as specifically addressed in previous pan-European efforts i.e. the European interoperability framework (EIF) and in ongoing development efforts on the European Open Science Cloud (EOSC) interoperability framework. In this document, we use the acronym EOSC-IF to refer to the EOSC interoperability framework draft.

The task's original plan aimed at producing results similar to the draft EOSC-IF. To avoid duplication of efforts, we modified the task's initial description of work and it was consequently approved by the EOSC-Nordic Project Management Board as well as Project Officer.

We aim to highlight how services can interrelate so as to deliver expected value to the users in cross-border contexts. We will attempt to describe the elements that should be addressed in order to achieve better alignment and interoperability of services. Our objectives are as follows:

- Support Nordic and Baltic service providers in enhancing the interoperability of services in cross-border environments;
- Contribute to ongoing discussions towards the development of the EOSC interoperability framework.

The observations outlined in this document aim at giving a general approach for improving interoperability across services in the Nordic and Baltic regions. The approach is subject to improvements and updates in response to ongoing developments related to the EOSC interoperability framework.

I.2 Definitions

In order to maintain an alignment with EOSC-IF, we adopt the general definition of interoperability as outlined in the EOSC-IF -

Interoperability: A characteristic of an Information Technology (IT) system, whose interfaces are completely understood, to work with other IT systems, at present or in the future, in either implementation or access, without any restrictions.

The FitSM standard for lightweight IT service management defines a service as follows -

Service: A way to provide value to customers through bringing about results that they want to achieve. Please note that when referring to services, usually IT services are meant.

1.3 How to read this deliverable

This document is structured as follows:

- Section 2 outlines a general overview of interoperability frameworks.
- Section 3 describes the recommendations selected for analysis, together with the methodology applied and the analysed cases.
- Section 4 provides a summary of the main observations based on the analysis done on case services, including our view on how this work could contribute to the ongoing developments towards an operational EOSC.
- Section 5 concludes the report.

2. Interoperability Frameworks

This section presents an overview of the interoperability frameworks. Generally, interoperability frameworks are composed of guidelines serving as foundations for more detailed enterprise architecture and development work.

2.1 European Interoperability Framework

The European interoperability framework (EIF) provides guidelines aiming to enhance interoperability of IT services. The EIF website states that

*The European Interoperability Framework (EIF) is part of the [Communication \(COM\(2017\)134\)](#) from the European Commission adopted on **23 March 2017**. The framework gives specific guidance on how to set up **interoperable digital public services**. It offers public administrations 47 concrete recommendations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts.*¹

In this deliverable, we refer to the second (and most recent) version of the framework, simply called the 'new EIF'.² It defines basic interoperability guidelines in terms of principles, interoperability layers, models and recommendations. As mentioned above, the EIF document discusses public services, not interoperable IT services for research activities.

The first 19 recommendations cover interoperability principles that are grouped into the following sets:

1. Principle setting the context for EU actions on interoperability
2. Core interoperability principles
3. Principles related to generic user needs and expectations

¹ https://ec.europa.eu/isa2/eif_en

² https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

4. Foundation principles for cooperation

In addition to these, there are 14 recommendations focusing on the interoperability model (Figure 1), which includes the four layers and their governance:

1. Technical interoperability
2. Semantic interoperability
3. Organisational interoperability
4. Legal interoperability

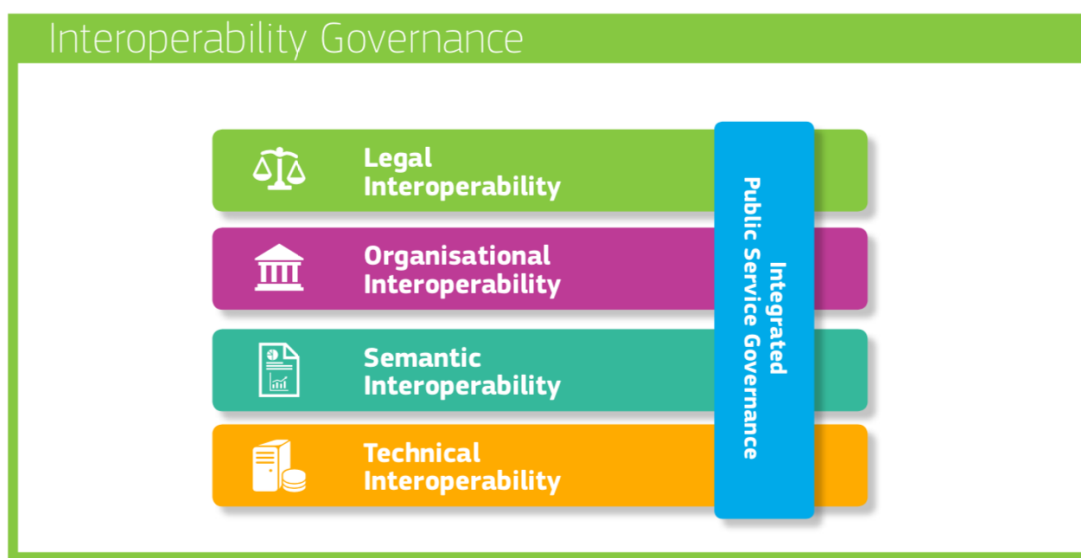


Figure 1: Interoperability model⁴

The last 14 recommendations cover the conceptual model that provides guidance for planning and developing integrated public services.

It should be noted that there is no single audience for the EIF recommendations. Some of the recommendations are targeted to national policy makers, and some can be taken into account by service providers.

2.2 EOSC Interoperability Framework

As discussed above, the EIF was not targeted for research communities. In order to promote interoperability within EOSC, the FAIR working group of the EOSC secretariat³ released a draft version of the EOSC interoperability framework.

The EOSC-IF was mainly tailored from EIF and is therefore not a one-to-one mapping. The current draft concentrates mostly on data and related research artefacts. Legal interoperability issues will be considered in the next version of the document. We also expect the next version to contain more discussion about services.

³ <https://www.eoscsecretariat.eu/sites/default/files/eosc-interoperability-framework-v1.0.pdf>

3. Selected recommendations

3.1 Methodology

We used the European interoperability framework as a starting point. We first listed the principles, interoperability layers and the conceptual model along with the corresponding recommendations in a Google sheet. Next, we looked at the EOSC interoperability framework, paying attention to the similarities and differences in the recommendations within both frameworks. Then we proceeded by iteratively discussing the recommendations and selected those considered to be applicable to services. The EOSC-IF “provides general recommendations for achieving interoperability across services (e.g., interoperability in authentication and authorisation, interoperability in the exchange of data, interoperability for ensuring the findability of resources)...” Here, we focused on selecting recommendations that would enable more alignment in achieving interoperability of EOSC-related services.

In addition to the four layers of interoperability described by EIF, and consequently adopted by EOSC-IF (technical, semantic, organisational and legal), we also considered recommendations covered under other underlying principles (subsidiarity and proportionality, openness, transparency, reusability, technological neutrality and data portability, user-centricity, inclusion and accessibility, security and privacy, multilingualism, administrative simplification, preservation of information and assessment of effectiveness and efficiency) and the conceptual model of the EIF. The goal was to focus on recommendations that would improve service interoperability across services providers, considering diversity of providers and services themselves. Overall, we selected recommendations based on a common understanding of the recommendations’ relation to service-related concepts (e.g. service management, service architecture and design, service operations, accessibility, processing of research data). This exercise resulted in 21 recommendations.

Next, we used the selected recommendations as a basis for formulating questions intended for assessing the services. The purpose of the questions was to convert the ideas in the recommendations into expressions that would be comprehensible and potentially easy to answer. The questions were intended for service providers, because they are normally responsible for the services during different phases - design, development, production etc. We used an iterative process, during which each team member was responsible for composing the initial questions from a subset of the recommendations. The rest of the team then reviewed the questions and provided suggestions for improvement. In order to capture the essence of the recommendations while minimising loaded and run-on questions, it was appropriate to use more than one question for some of the recommendations. As a result, we generated 35 questions out of the 21 recommendations (See 3.2 below).

3.2 Recommendations, questions and the reasoning for their selection

As we previously stated, we considered the recommendations originating from EIF and followed its interoperability model while paying attention to the EOSC-IF.

We have not explicitly considered the first principle of Subsidiarity and Proportionality, since this is directed to the EOSC’s position on interoperability, rather than services and their providers.

3.2.1 Core interoperability principles

European Open Science Cloud has its foundation in Openness. And we started with this principle when considering recommendations and formulating questions targeting concepts of open data, open software and open specifications. Services should not hinder or limit openness but at best promote and facilitate it. *Openness*, together with *Technological neutrality* and *data portability*, *Transparency* and *Reusability* are considered to be **Core interoperability principles**.

Avoiding the risk of vendor lock-in and technology specific solutions, and assuring data portability is the way to increase interoperability between services. Big tech companies (Google, Microsoft, Apple, Facebook, Twitter) are also looking into increasing their service interoperability by creating an open-source, service-to-service data portability platform⁴. This shows that some of the interoperability aspects are still challenges demanding global solutions.

Table 1: Core interoperability principles

Recommendations	Questions
<p>Publish research outputs openly unless certain restrictions apply (“as open as possible, as closed as necessary”).</p> <p>Ensure a level playing field for open source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.</p> <p>Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.</p> <p>Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.</p> <p>Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of EOSC services without unjustified restrictions, if legally possible.</p>	Do the users control the openness of their data without limitations from the service?
	If your service contains proprietary software/components, can you ensure reuse of data without proprietary tools?
	If your service contains proprietary software/components, can you ensure reproducibility of the results?
	Does your service rely on open specifications (e.g. APIs, data models) that are relevant for the end users?
	In using your service, is there a risk for vendor lock-in effects for the users with respect to the technology (e.g. architecture, licensing, proprietary components, hardware) used in your service?
	Does your service support easy transfer of data with external services and applications?
	Does your service provide datasets with well-defined metadata that can be used by other services?

⁴ <https://datatransferproject.dev/>

	Does your service provide APIs that can be used by other services?
--	--

3.2.2 Generic user needs and expectations

The main purpose of services is to produce value for researchers using them. So, this group includes **principles related to generic user needs and expectations**. *User-centricity, Security and Privacy, Inclusion and Accessibility* and *Multilingualism* are important criteria to increase interoperability. We formulated the questions in such a way that would help us understand if service providers consider these aspects when operating the services.

Table 2: Generic user needs and expectations

Recommendations	Questions
Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.	Does your service have a single point of contact that end users can use for service requests?
Put in place mechanisms to involve users in analysis, design, assessment and further development of EOSC services.	Do you have formalized feedback mechanisms to involve users e.g user surveys, advisory boards, etc?
Ensure that all EOSC services are accessible to all research organizations, researchers, citizens, including persons with disabilities, the elderly and other disadvantaged groups. EOSC services should comply, as much as possible, with e-accessibility specifications that are widely recognised at European or international level.	Does your service comply with the accessibility directive?
	Does your service currently support multiple languages?
	Does your service have a roadmap for supporting multiple languages?
Use information systems and technical architectures that cater for multilingualism when establishing an EOSC service. Decide on the level of multilingualism support based on the needs of the expected users.	Have you analyzed your end-users' needs for multilingualism support?
Define a common security and privacy framework and establish processes for EOSC services to ensure secure and trustworthy data exchange between all involved parties.	Do you have a documented and implemented policy to ensure that services are secure and trustworthy? One example of such a policy would be e.g. set of requirements based on ISO/IEC 27000.

3.2.3 Legal interoperability

We are assuming that services provided through EOSC are by nature cross-border, and that service providers are aware of existing legislative requirements. This will increase the need for **legal interoperability** and in particular service providers dealing with personal and sensitive data will be required to have a deep understanding of all legal implications⁵. We expect services to support and assist users in following regulations and legislations.

Table 3: Legal interoperability

Recommendations	Questions
Ensure that legislation is screened by means of 'interoperability checks', to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a 'digital check' and consider data protection requirements.	Does your service obtain consent from users before publishing or sharing information about users or the users application of your service?
	Does your service transparently describe and enforce limitations on users right to access, share, or make use of users data or business logic developed by the user? Such limitations may be in the form of transaction fees when the user accesses, shares or makes use of data. Limitations may also be in the form of automated transfer of intellectual property rights from user to service owner when user uploads, shares, processes or transfers data.

3.2.4 Technical and organisational interoperability

Integration of services which operate across borders require multilateral or global agreements. Service providers need to align their own processes, responsibilities and expectations to achieve commonly agreed goals. The relationships between service providers and service consumers must also be clearly defined. Here, we chose three recommendations from the **technical interoperability** layers and one from the **organisational** layer.

Table 4: Technical and organisational interoperability

Recommendations	Questions
Use open specifications, where available, to ensure technical interoperability when establishing EOSC services.	Does your service openly describe how to use the APIs of the service?
Coarse-grained and fine-grained dataset (and other	Does your service describe how to set metadata on files or data processed through the service?

⁵ EOSC-Nordic D2.3: Open Science in the Nordics: Legal Insights - <https://zenodo.org/record/4147409#.X6p3oVVMQ2x>
11

<p>research object) search tools need to be made available. There will be a range of general-purpose and domain-specific/specialised search tools, exploiting general-purpose and domain-specific metadata.</p> <p>The Service-Level Agreements for all EOSC resource providers should be easy to understand by users from different communities</p>	Does your service support APIs or search tools to enable searching of metadata?
	Do you have an SLA for your service?
	Is your SLA easy to understand?
Clarify and formalise your organisational relationships for establishing and operating European public services.	Does your organisation have a process for or experience with establishing and terminating formalised organisational relationships with other partners with whom you develop and operate joint services?

3.2.5 Semantic interoperability

The last layer in the interoperability model, is **semantic interoperability**. It is concerned not only with the packaging of data (syntax), but also the simultaneous transmission of the meaning of the data (semantics). This is accomplished by adding data about the data (metadata), and linking each data element to a controlled, shared vocabulary.

Table 5: Semantic interoperability

Recommendations	Questions
Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.	Does your service support easy access to different data and metadata formats?
	Does your service support integration of data with different formats and from different sources?

The European interoperability framework and the European interoperability architecture (EIRA) are important parts of *Interoperability Governance* which is the key to a holistic approach on interoperability, as it brings together all the instruments needed to apply it. As such, the recommendations related to *Interoperability Governance* are beyond the scope of this deliverable. Instead, they should be considered by the EOSC Architecture working group / EOSC Governance body.

3.2.6 Conceptual model

We conclude our selection of recommendations and questions from the **conceptual model**⁶ for a common approach on integrating services.

Table 6: Conceptual model

Recommendations	Questions
Create and follow data quality assurance plans for base registries and related master data.	Do you create and follow data quality assurance plans for widely used datasets?
Publish open data in machine-readable, non-proprietary formats. Ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.	Do you have a policy to ensure that your service produces correct results within technical and technological limits?
	Does your service support data publishing in open formats, with no restrictions upon usage following the FAIR principles?
	Does your service support datasets with machine-readable metadata?
Communicate clearly the right to access and reuse open data. The legal regimes for facilitating access and reuse, such as licences, should be standardised as much as possible.	Does your service support metadata in open formats?
Use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services.	For each dataset, do you clearly state the licensing of that dataset? For instance that this dataset is licensed under Creative Commons, GPL, BSD?
	If yes, do you specify e.g. the version and/or more detailed license type?
Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans.	Do you have risk management plans in place, taking into account security and privacy measures?
	Do you use electronic identification (eID) and/or other trust services (e.g. e-signatures, e-timestamps, e-seals etc) as mechanisms to ensure secure and protected data exchange?
	Do you use other similar services as mechanisms to ensure secure and protected data exchange?

⁶ The conceptual model promotes the idea of interoperability by design. It means that for European public services to be interoperable, they should be designed in accordance with the proposed model and with certain interoperability and reusability requirements in mind.

3.3 Service case studies

In order to put the aspects related to service interoperability in context, we selected six services with the aim of providing a set of observations. The observations help the community with a general understanding of the applicability and suitability of our method on addressing service interoperability. The service types are as follows:

- 3 cases are HPC services provided by national e-infrastructure providers: **UT Rocket** - Estonia; **Puhti** - Finland; **RTU HPC** - Latvia
- 2 cases are data management services: **Danish National Archives** - Denmark and **Fairdata services** - Finland
- One case (**Puhuri**) is a new service currently being developed to handle LUMI⁷ user and resource management. Puhuri is in the requirements collection and technology architecture planning phase, and thus not yet fully defined and implemented.

All the cases are potential EOSC services. Although they are not exhaustive across geographic coverage or service types, they are meant to highlight general service interoperability issues that are important in cross-border contexts, and EOSC at large.

4. Analysis

In order to determine the state of the interoperability of services, a subset of the existing service providers were selected to analyse their services from an interoperability perspective. We used a questionnaire containing the questions in 3.2 as our data collection tool. There were four options for answering a question (Yes, No, Unknown & N/A) along with the additional possibility to provide an explanation for the answer, if necessary. We invited the service owners responsible for the six services to respond to the questionnaire.

Due to timing constraints the respondents of the survey i.e. the service providers, were given the option of answering the survey in either of two ways: (1) individually - with the option to ask for clarifications; (2) in an interview with one or two members of the task team.

The choice of which option to use was up to the service providers. Three services were assessed using option one, and the remaining three with the second option.

It shall be noted that, providing clarifications remotely and/or during the interviews helped us to minimise potential misunderstandings.

The analysis covers three service categories in the Nordic and Baltic countries. 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. The service categories included in the analysis are repositories, compute services, and service aggregation solutions.

⁷ <https://www.lumi-supercomputer.eu/>

4.1 Findings

The responses to the individual questions from our questionnaire were calculated in each of the 6 interoperability groups. The results were then presented in a matrix showing the 6 individual services in the columns of the matrix and the 6 interoperability groups in the rows of the matrix. An average compliance level was calculated by dividing the sum of results with the number of services. This was presented on the last row of the matrix. Similarly, an average compliance level on the 6 individual interoperability groups was calculated and shown on the last column.

As shown in Figure 2 below, the compliance levels differ greatly from service to service and between our 6 interoperability groups.

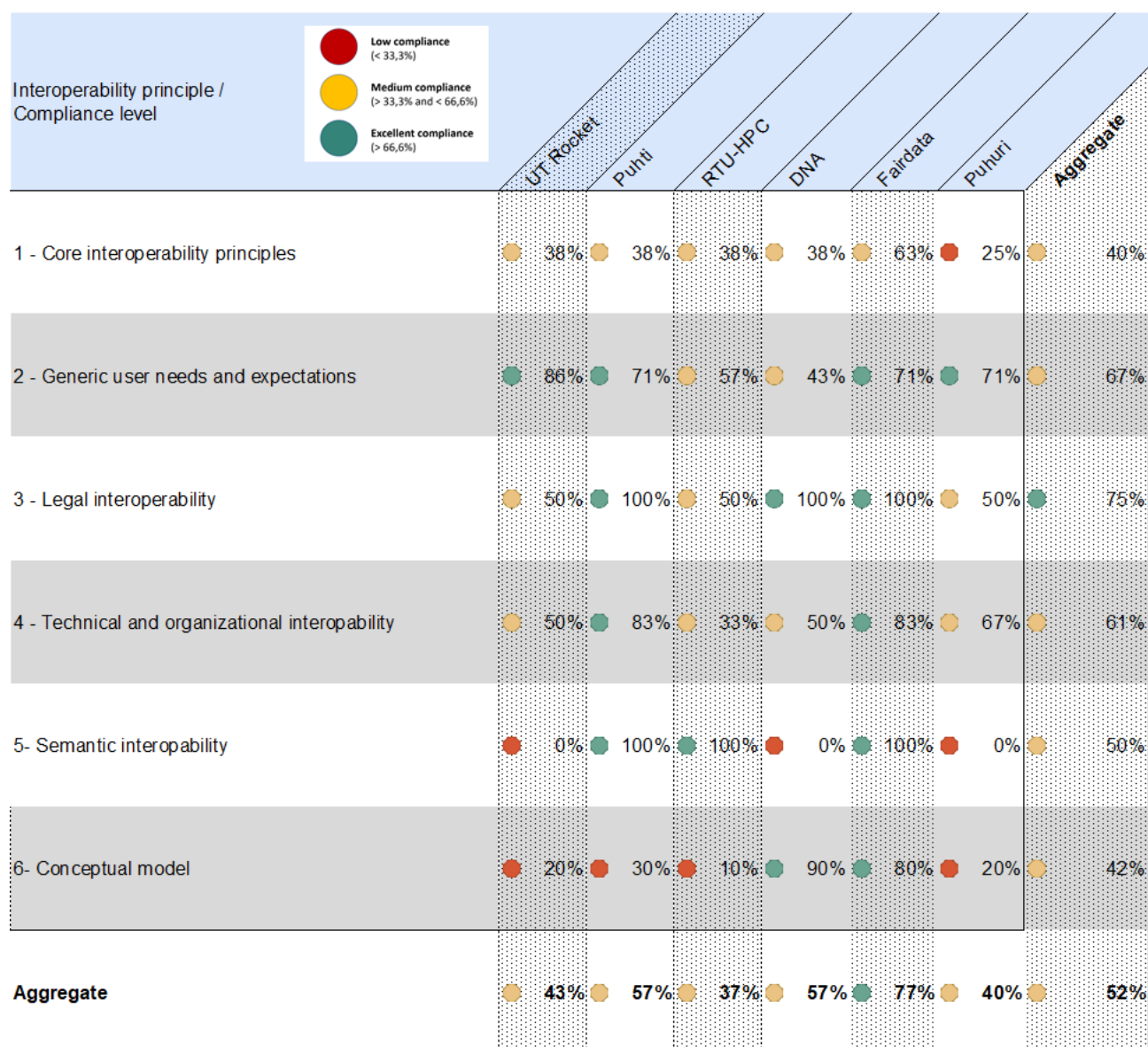


Figure 2: A matrix showing the calculated degree of compliance by each service in relation to the interoperability principles

The matrix shown above presents the calculated degree of compliance based on the responses to our questionnaire. The individual results for each service were calculated as a sum of all responses to all questions submitted in the individual interoperability principles. For instance, the result of 38% for “Core interoperability principles” for “UT-Rocket” was calculated as a sum of all UT-rockets positive (i.e. ‘yes’) responses to the questions under the group “Core interoperability principles” and then divided this sum by the number of questions (8) covered by that group.

4.1.1 Core interoperability principles

The services achieved a medium overall result on the core interoperability principles, and a high degree of compliance on use of open APIs. They also achieved a low degree of compliance on questions pertaining to reusability of and reproducibility of results. This may be due to misinterpretations of questions and use of proprietary tools and formats that are determined by user behavior and not by the functionality of the service.

In a few cases, the low degree of compliance on reusability and reproducibility of results was due to the service provider’s awareness of potential user behaviour as a barrier to reusability of data and reproducibility of results. This could be the case if users could choose to make use of proprietary formats and tools. Our questions were aimed at identifying the degrees of compliance, and fortunately, the comments from the service providers were also able to identify user behaviour as a potential root cause for the low degree of compliance.

This raises questions of whether the individual service providers should discourage or even disable use of proprietary data and tools. On the other hand, regulating such behaviour could easily be seen as a radical intervention that reduces usability and flexibility for its users. However, reusability and reproducibility are core elements of interoperability in general and FAIR in particular. Therefore, identifying, analyzing and making balanced recommendations on reusability and reproducibility are highly recommended for further work.

4.1.2 Generic user needs and expectations

The services achieved a high degree of compliance with these interoperability principles. This is especially the case on questions pertaining to the administrative setup of the service. The questions included in this group covered several interoperability issues concerning user-centricity, security and privacy, inclusion and accessibility and multilingualism. The highest levels of compliance were measured on user-centricity (83%). The lowest levels of compliance were measured on questions regarding security and privacy (50%). Responses to questions regarding inclusion and accessibility achieved a good level of compliance (67%), and multilingualism also received a good level of compliance (61%).

4.1.3 Legal interoperability

The services achieved a high degree of compliance with these principles. The questions were mostly directed towards enabling digital sovereignty for users. All services gather user consent when relevant, while only half of the services transparently describe issues pertaining to digital sovereignty.

4.1.4 Technical and organisational interoperability

The services achieved a high degree of compliance with these principles. This is reflected in compliance with formal organizational relationships, while questions regarding the use of APIs result in lower compliance and questions regarding SLA result in almost full compliance.

4.1.5 Semantic interoperability

The services achieved 50% compliance on both questions regarding semantic interoperability. They were either fully compliant or non-compliant to the questions. The type of services complying to the questions seemed to be the deciding factor. Repositories were generally compliant while the other types of services were not.

4.1.6 Conceptual model

This category contained the highest number of questions. The results were very mixed. Two services were mostly compliant to the questions while four services were mostly non-compliant. The services were mostly compliant when the questions were directed towards specific security measures. When questions were directed at data formats and licensing terms, the services turned out to be mostly non-compliant.

These mixed results may be partially due to differences in service types and due to the inherent difficulties in distinguishing between interoperability compliance that is determined by the service and interoperability outcomes that are determined by potential end user behaviour.

As mentioned in 4.1.1. on core interoperability principles, several comments from the service providers indicated that some responses included user behaviour in their response, while others did not. The same difficulties apply to some of the questions covered in the conceptual model.

Our questions were mainly aimed at measuring compliance and not the root causes to compliance or non-compliance. Therefore, some of our questions may have been seen as ambiguous by the service providers. We did not specifically ask the service providers to include or exclude user behaviour in their responses. Therefore some service providers may fully enable users to be compliant to all questions regarding reusable data models, data formats and metadata, but still respond as non-compliant. This can be due to a single user of their service who chose behavior that was non-compliant. This raises several interesting questions:

1. To what degree should the service provider entice its end users to behave in ways that ensure compliance?
2. Where would a service provider gather recommendations for compliance that would be understandable and operational for end users?
3. Can non-compliant end user behavior even be identified or measured?
4. Should or could such behaviour be enforced by the service provider or by a neutral governing body?
5. Would it even be possible to examine user compliance while respecting data integrity and privacy?

These questions should be addressed in any further work concerning end-to-end compliance to the service interoperability framework. Clarifications on whether end user behaviour should be in scope for service providers ought be made before embarking on future surveys on IF compliance.

4.2 Reflections on responses from service providers

The questions answered by the 6 service providers were composed in order to examine the interoperability principles discussed in sub-section 3.2. With few exceptions, the intentions of our questions seem to have been clearly understood by the service providers. However, a few questions were unclear when applied in practice, leading to unexpected responses or misinterpretations.

4.2.1 Should end-user behavior be in scope?

A couple of our questions identified some misinterpretation of the scope of our analysis. The service providers seemed unable or unwilling to distinguish between compliance issues that were directly related to the features of the service and actual outcomes that were due to user behaviour. This was the case in several responses when examining the use of proprietary software and data formats. The actual use of open software and formats may for instance be greater than our findings indicate. A service provider may have developed a solution fully based on open software and formats and end up replying “no” when asked about these characteristics. For instance users of the service may in some cases store and make use of Microsoft Excel spreadsheets when using the service. This is a proprietary and licenced program with proprietary file formats.

The impact of such potential misunderstandings is expected to be limited to just a few responses. However, we cannot be sure if the service provider is aware of the extent of end-users who likely practice non-compliant behaviour, when in the data lifecycle such non-compliant behaviour is most likely to occur or whether particular groups of end-users are more likely to exhibit non-compliant behaviour. End users may not be aware that they are practicing non-compliant behaviour. They may not also be aware of available alternative and compliant methods or tools or may not care if they are compliant to any IF recommendations.

But before any of these kinds of questions can be addressed, the service providers will most likely have to decide whether end user behaviour is even something they wish to have in scope. If not, then the identification root causes of non-compliant end-user behaviour and any recommendations on compliant behaviour will have to be produced and governed by someone else.

4.2.2 Do one-size-fits-all questions apply?

The six services represent three categories of services, with varying mixes of service portfolio; HPC, data repositories, and aggregation services. The individual services were naturally only able to reflect on the interoperability issues that their particular service may have been exposed to. The fact that we have a slightly disjunct set of respondents limits the conclusions that may be drawn from the survey. In particular, it is not strictly possible to create a “single number measurement” on the compliance across the complete set of services, which would have been desirable in order to give an easy assessment on the level of compliance to the reader.

For example, many of our specific questions may have had limited or no impact on some services. In other cases, the issues were assessed to be outside of the realm of control of the service provider which is why the respondent was able to answer “not applicable” or “no” to our questions. Fortunately, many of the service providers expanded on their negative replies and stated the reasoning for this in their comments. Unfortunately, the analysis may show a low degree of compliance for some services even when they are mostly compliant on all the issues that currently have relevance or impact on the service.

However, although this does make the single-number measure aspiration unattainable, this does not make the common measurements irrelevant across these service categories. The upside of working with a model that encompasses many or all service types seem to outweigh the downside due to lack of tailored approaches to the service categories.

4.2.3 Will future user requirements increase the importance of interoperability frameworks?

Awareness of all the interoperability issues may currently be out of scope for some of the service providers. Some interoperability issues may be less relevant today but have a long-term impact on the future of the service.

The highest degrees of compliance amongst the services may be due to careful planning and governance by the particular service provider or the need of the particular service provider to accommodate advanced requirements by end users. The maturity of the service may also be influential. If a service has been in operation for many years and has had deep interaction with its end-users, the more exposure it will likely have had to interoperability issues.

Some services may also already overlap the categories due to advanced end-user requirements. This could be the case if a HPC service offers repository-like services for short-time storage or a repository offers users access to limited compute services. If future development of the services take a user-centric approach, we can expect even more overlaps across categories.

4.3 Recommended further work

Our work in composing and executing the analysis has led to several reflections on possible improvements and further work. These reflections lead to the following recommendations:

1. **Two parallel analysis tracks.** The effect of service provider features and end-user behaviour has been difficult to separate. Practical interoperability should take both aspects into consideration. Further study of end-user behaviour on the individual services is expected to lead to more clarity on how practical interoperability could be achieved.
2. **Removal of overlapping questions.** A handful of our questions include overlapping issues. For instance the availability of API's is addressed through two questions and a few questions concerning the conceptual model seem to get copy/paste responses. This might indicate redundancy amongst these questions.
3. **Improvements on unclear questions.** For instance, we have a question concerning the choice of licensing models for datasets. This question could focus on whether the service requires purchase of third party software licenses by end-users or future software license renewals that may affect the service provider or its end-users. There is also a need to have a common meaning of the 'yes/no' answers over all the questions e.g. in asking about the risk of vendor-lock in, answering 'no' was actually a good thing, even though it was having a 'yes' that counted towards compliance to the question.

4. **Enhanced focus on metadata.** Compliance with FAIR through interoperability could be a relevant future focus point. This could be achieved by examining the generation and traversal of metadata through the use of standardised communication protocols, service tools, repositories and compute services. Metadata should be either maintained or enriched during this process.
5. **Examination of more services.** More responses would enable compiling an analysis that is less influenced by one or more services that may be atypical.
6. **Compilation of relevant baselines or “golden standards”** that cover interoperability for repositories, compute services and/or service aggregators. This could be a tool to indicate what an individual service could or should strive to achieve.
7. **Build a more coherent IF.** Moving from general recommendations produced by various authors and with various intentions to specific questions aimed at measuring compliance was naturally difficult. Further mapping between IF recommendations from various sources would be helpful and bring much needed clarity.

4.4 Relation to EOSC development

As discussed earlier, many EIF recommendations were left out of our analysis. This is mainly because it is difficult to take them into account in the context of services. Many of the dropped recommendations are more relevant for high-level EOSC governance. As the development of EOSC takes operational steps, we can expect to have further guidance for development of existing services, taking into account interoperability issues relevant for EOSC.

As a first step, to enhance interoperability of EOSC services, EOSC actors and their tasks should be clarified. More specifically, a functional EOSC service management system taking care of daily operations should be clearly defined. Another step would be for the EOSC architecture governing body to become the “nexus” of EOSC service design governance ensuring that EIF and EOSC-IF recommendations will be realized in more detailed guidelines and policies.

The questions we have developed may contribute towards interoperability efforts across EOSC, and especially in the context of improving interoperability across the services. Therefore, this work complements the work of the FAIR Working Group in achieving interoperability during EOSC’s development.

4.5 Summary

The analysis has shown mixed results from the individual services concerning compliance to the interoperability issues we have chosen to include in the analysis. Such a mixed result could be worrying if only taken at face value. Fortunately, we have identified a high degree of awareness, insight, and responsiveness of the interoperability issues on the part of the service providers. Therefore, the analysis has been able to incorporate comments and reflections made by the service providers and take these into account.

Our analysis indicates that the services achieve an overall medium level compliance to the interoperability principles.

Our work has brought us closer to identifying which types of services are expected to be compliant with which type of interoperability principles. However, we are not yet at the stage where we can determine whether the analysis results are satisfactory. For this to be determined we would need comparative results derived from previous similar analysis. Unfortunately, such previous analyses do not exist. Therefore we are not able to determine whether the degree of compliance we have identified is as expected, lower than expected or better than expected.

The analysis does potentially plot a course for the service providers themselves to identify areas that could improve. The analysis itself could also be improved. This could be achieved by delivering more clarity on its scope (features and/or end-user behaviour) and rephrasing questions that in some instances seem to be misunderstood by the service providers.

5. Conclusions

Interoperability issues are usually complex, often requiring consideration from different viewpoints. Despite the complexities, the service providers demonstrated a high degree of awareness, insight, and responsiveness of the interoperability issues. The reflections made by the service providers are useful for achieving interoperability in practice. The development of interoperability frameworks should leverage on engagement with the right stakeholders e.g. service providers, end-users, policy makers, funders etc.

Comparing different types of services using a homogenous set of questions is difficult because of the unique characteristics among the services. In future, this may be solved by conducting analyses in the context of each service type and/or user base. Such comprehensive evaluations for further development would require high degrees of coordination.