D5.4 EOSC Core Innovation Sandbox

30/09/2025

Abstract

The document provides a detailed description of the EOSC Core Innovation Sandbox and its access model, outlining how users and providers can engage with the platform. Additionally, it includes an initial report on the integration processes involving external providers, offering insights into the functionality achieved through these integrations.

Funded by the European Union

EOSC Beyond receives funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101131875

Document Description

Document title			
Work Package number			
Due date	30/09/2025	**Actual delivery date:**	08/10/2025
Nature of document	Report	**Dissemination level**	Public
Document Status	Under EC review	**Version**	1.0
Lead Partner	IPB		
Authors	Dusan Vudragovic (IPB), Anastas Mishev (UKIM)		
Reviewers	Athanasios Mantes (ATHENA), John Shepherdson (CESSDA ERIC)		
Approved by	TCB		
Document link	https://documents.egi.eu/document/4116		
DOI	https://zenodo.org/records/17292990		
Keyword	EOSC, sandbox, providers, services, access, node		

Revision History

Issue	Date	Description	Author/Reviewer
V 0.1	07/02/2025	Initial ToC	Dusan Vudragovic (IPB) Anastas Mishev (UKIM)
V 0.2	08/26/2025	Revised version	Dusan Vudragovic (IPB) Anastas Mishev (UKIM)
V 0.3	09/18/2025	Revised version	Dusan Vudragovic (IPB) Anastas Mishev (UKIM)
V 0.4	09/24/2025	Revised version	Dusan Vudragovic (IPB) Anastas Mishev (UKIM)
V 0.5	07/10/2025	Corrections	Nicola Fiore (EGI), Diego Scardaci (EGI)
V 1.0	**08/10/2025**	**Final**	

Table of content

Figures

Tables

Executive Summary

The EOSC Beyond Innovation Sandbox is a pre-production environment where researchers, service providers, and node operators can test and integrate the latest EOSC Core developments in a safe, controlled setting. It reduces risks before production by validating interoperability, ensuring compliance with EOSC standards, and supporting integration of new nodes and services.

Functioning as a Federator Node for project pilots, the Sandbox offers Core Federating Capabilities as the foundation for testing. These include secure federated access through the Authentication and Authorisation Infrastructure (AAI), workflow deployment via the Execution Framework, and operational support through Helpdesk, Messaging, Monitoring, and Accounting. Persistent Identifier (PID) services guarantee long-term traceability of digital objects, while the Resource Catalogue, Order Management, and Front Office provide structured access to services and data. Standardised adapters simplify interoperability across diverse resources, lowering technical barriers for providers.

The Sandbox supports multiple user groups: service providers can validate datasets, tools, and services; research communities can test workflows and FAIR data practices; and infrastructure operators can assess node deployment and interoperability. Access requires a streamlined enrollment or onboarding process that ensures legal accountability, metadata compliance, reliable delivery, and basic support—maintaining quality while encouraging experimentation.

Extensive guidance is provided through the **Sandbox Documentation Hub**, which delivers task-oriented resources for pilot nodes, providers, and developers. This supports users at all levels in effectively interacting with the EOSC infrastructure.

The Sandbox is already operational, having validated multiple integrations of EOSC Core Federating Capabilities and demonstrated the robustness of the federated approach. Pilot nodes (CESSDA, CNB-CSIC, e-INFRA CZ, ENES, INSTRUCT-ERIC, LifeWatch ERIC, METROFOOD-RI, NFDI, NI4OS-Europe) successfully tested services such as AAI, Helpdesk federation, and automated deployment. These highlighted strengths alongside areas needing refinement, including documentation, service maturity, and template quality.

Future plans include extending automation of integration, enrollment, and onboarding, broadening access to more providers and communities, and using the Sandbox as the primary validation tool for EOSC Nodes. By promoting interoperability and reducing integration risks, the Sandbox strengthens the stability, scalability, and innovation capacity of EOSC, reinforcing Europe's Open Science ecosystem.

1. Introduction

This document provides a comprehensive overview of the EOSC Core Innovation Sandbox, a key result of the EOSC Beyond project. The Sandbox is designed as a pre-production environment to facilitate the development, testing, and integration of Pilot Nodes and services.

1.1. Purpose of the document

The primary purpose of this deliverable is to formally describe the EOSC Core Innovation Sandbox. It details its architecture, core components, and the operational model that governs its use. Furthermore, this document establishes the access models for various stakeholders, including EOSC Core and Exchange service providers. Finally, it serves as the initial report on the integration activities, documenting the progress of core and external providers who have utilized the Sandbox environment.

1.2. Scope of the document

The scope of this document is focused on the Innovation Sandbox as a testing, staging, and service incubation environment. It covers the technical design of the Sandbox, its constituent services, and the processes for gaining access and integrating resources. The document also includes a preliminary report on the integration of services that have taken place during the initial phase of the project. It does not extend to the operational details of the final EOSC production environment, but rather the pre-production platform designed to ensure software quality and successful integration prior to live deployment.

1.3. Structure of the document

This document is organised into five chapters, each addressing a specific dimension of the EOSC Core Innovation Sandbox:

- **Chapter 2** – Role of the EOSC Core Innovation Sandbox introduces the concept of the Sandbox, explaining its definition, its objectives for the EOSC Federation, the stakeholders it addresses, and the expected impacts.

- **Chapter 3** – The EOSC Core Innovation Sandbox presents the implementation of the Sandbox as a fully operational environment and introduces its dedicated landing page designed for different stakeholder groups. It explains how users engage with the Sandbox through specific access models and onboarding procedures, and describes the requirements for providers and services wishing to participate. The chapter also details the process for deploying and validating EOSC Pilot Nodes within the Sandbox.
- **Chapter 4** – First integration report provides an overview of the initial integration activities carried out by Pilot Nodes and providers. It summarises their experiences, highlights strengths and challenges, and extracts lessons learned from the first

testing cycle.

- **Chapter 5** – Conclusions and next steps summarises the main achievements of the Sandbox to date and sets out the future roadmap, including planned enhancements, extended access, and the role of the Sandbox in validating EOSC Nodes and showcasing new capabilities.

- **Annex 1** – Components and services offers detailed technical descriptions of the Sandbox components, including AAI, Execution Framework, Helpdesk, Messaging, Monitoring, Accounting, PID, Resource Catalogue, Order Management, and the Front Office.

2. Role of the EOSC Core Innovation Sandbox

2.1. Definition of the EOSC Core Innovation Sandbox

The European Open Science Cloud (EOSC) has been conceived as a federated environment that connects services, tools, data, and computing resources across Europe. Its overarching goal is to enable researchers to discover, access, and reuse scientific outputs seamlessly and to foster a sustainable digital ecosystem that supports multidisciplinary collaboration and strengthens Europe's position in Open Science.

Within this broader vision, the EOSC Beyond project plays a key role by extending the EOSC Core with new technical capabilities and by establishing the foundation for a network of pilot EOSC Nodes at national, regional, and thematic levels. Among the project's Key Exploitable Results (KERs), the EOSC Core Innovation Sandbox (KER2) addresses a long-standing challenge in digital research infrastructures: ensuring that new services and components are both reliable and interoperable before being released to a wide community of users.

In the early stages of EOSC, integration activities were often constrained by fragmented and inconsistent testing environments. Providers and Node operators lacked a trusted space where they could safely experiment, validate, and troubleshoot integrations before moving to production. The Sandbox was therefore designed as a dedicated pre-production environment to close this gap.

It offers a controlled and federated space where EOSC Core providers can introduce new functionalities, where external service providers can verify compliance with EOSC standards, and where Node operators can prepare their infrastructures for federation. Acting simultaneously as a technology testbed, service incubator, and training environment, the Sandbox provides a structured and transparent pathway from innovation to production readiness.

By formalising this process, EOSC Beyond ensures that integration becomes a consistent, quality-assured activity rather than an ad-hoc or risky step. The Sandbox thus embodies the core principles of EOSC — openness, interoperability, and collaboration — while ensuring the stability and sustainability of the European Open Science ecosystem.

2.2. Objectives for the EOSC Federation

The EOSC Core Innovation Sandbox functions not only as a technical environment but also as a strategic instrument to strengthen the long-term vision of the EOSC Federation. Its design responds to the need to balance openness and innovation with quality control and interoperability across a diverse landscape of services and infrastructures.

A central objective is risk reduction. By shifting integration and validation activities from the production system to a pre-production environment, the Sandbox allows providers and Node operators to detect and resolve issues early. This approach safeguards the federation's stability while maintaining space for experimentation and continuous improvement.

Equally important is the goal of interoperability assurance. EOSC relies on shared frameworks such as the Authentication and Authorization Infrastructure (AAI), Persistent Identifiers (PIDs), metadata profiles, and FAIR data principles. The Sandbox acts as a Federator Node, offering a venue to test compliance with these frameworks and to ensure that connected services operate consistently within the federated model.

The Sandbox also supports service quality and compliance by providing mechanisms to validate the robustness, reliability, and FAIR alignment of services. This multidimensional testing ensures that resources onboarded into EOSC are ready for sustainable use by the research community.

Finally, the Sandbox contributes to capacity building within the federation. It allows Node operators — including emerging national, regional, and thematic infrastructures — to rehearse deployments, validate onboarding workflows, and strengthen their operational maturity before entering production. In doing so, it accelerates the creation of a coherent network of interoperable Pilot EOSC Nodes capable of sustaining the federation's growth.

Taken together, these objectives demonstrate how the Sandbox transforms integration into a strategic enabler of EOSC, supporting innovation while ensuring reliability, trust, and long-term sustainability across the federation.

2.3. Stakeholders of the Sandbox

The EOSC Core Innovation Sandbox has been designed to serve a broad spectrum of stakeholders, reflecting the diversity of the EOSC ecosystem. Each group benefits from the Sandbox in a specific way, while collectively contributing to the development of a more integrated and resilient federation.

For EOSC Core service providers, the Sandbox provides a controlled environment to test, validate, and enhance fundamental components such as AAI, Helpdesk, Monitoring, Accounting, and PID services. It enables them to ensure that new functionalities are interoperable and stable before they are introduced into production.

For EOSC Exchange service providers, the Sandbox acts as a gateway to the federation. By simulating the operational EOSC environment, it allows providers to verify that their datasets, computational services, and software tools meet the required standards for metadata, accessibility, and interoperability — all without exposing their users to the risks of early-stage deployment.

Research communities use the Sandbox to validate complex workflows that combine data and tools from multiple domains. By reproducing realistic federation conditions, the environment helps them ensure reproducibility, FAIR compliance, and cross-domain compatibility, encouraging collaboration and innovation.

For infrastructure operators — particularly those preparing to become EOSC Nodes — the Sandbox serves as a training and validation platform. Here, operators can test authentication

mechanisms, resource catalogues, and helpdesk integrations, allowing them to fine-tune their configurations and verify interoperability before joining the federation.

Developers and integrators use the Sandbox as both a laboratory and showcase. It provides APIs, adapters, and test datasets for developing and validating software components that facilitate integration between EOSC services. These reusable tools reduce technical barriers and strengthen the federation's interoperability fabric.

Finally, EOSC governance and policy bodies benefit from the Sandbox as a transparent and evidence-based mechanism to assess service quality, compliance, and readiness. Insights gathered from Sandbox operations help inform decision-making and the evolution of federation policies.

Through this collaborative and multi-stakeholder approach, the Sandbox operates not as a standalone facility but as a federated asset — a shared foundation for innovation, coordination, and trust-building across the entire EOSC landscape.

3. The EOSC Core Innovation Sandbox

The EOSC Core Innovation Sandbox is already in production and accessible online at **https://sandbox.eosc-beyond.eu**. It has been designed not as a theoretical prototype but as a fully operational environment, ready to serve the diverse categories of stakeholders engaged in the EOSC Federation.

Functioning as a virtual Federator Node, the Sandbox delivers the EOSC Core Federating Capabilities developed within EOSC Beyond, offering an authentic and controlled environment for testing interoperability across the federation. These capabilities—covering authentication and authorization, persistent identifiers, monitoring, accounting, helpdesk, messaging, execution framework, and resource cataloge—constitute the foundation of the EOSC and embody the essential technical building blocks of the EOSC Federation.

In particular, the Authentication and Authorization Infrastructure (AAI) provides secure federated access and single sign-on across nodes, while the Execution Framework supports the deployment and lifecycle management of applications through the Infrastructure Manager (IM) and TOSCA templates. Operational continuity is ensured by the Helpdesk, which federates support and ticketing, and by the Messaging Service, which enables reliable communication between components via the ARGO Messaging Service. Service reliability and usage are monitored respectively by the Monitoring and Accounting services, which collect, publish, and expose data on availability, reliability, and usage metrics. The PID Service guarantees long-term persistence and traceability of digital objects through globally resolvable identifiers.

For resource discovery and management, the Resource Catalogue integrates both services and research products, supported by dashboards for providers and onboarding teams. Complementing this, the Order Management System ensures a consistent process for requesting and provisioning resources, while the Front Office provides researchers with an intuitive entry point to the EOSC. Through its Explore interface, the Discovery Hub, and personalised User Dashboard, the Front Office offers seamless access to services, tools, and data across EOSC.

Thanks to these federating capabilities, pilot Nodes and service providers can test the enrolment and onboarding processes into the federation, experiment with interoperability mechanisms, and validate their configurations before moving to production. The Sandbox thus acts both as a reference implementation of the EOSC Core and as a training environment where pilot Nodes and providers can verify compliance with federation standards and procedures.

The complete list of EOSC Core Federating Capabilities is presented below:

Federating Capability	Core Component(s)	Function
Authentication and Authorization	AAI (Infrastructure Proxy, Identity Hub, Federated AAI Connector)	Federated access across nodes and services, single sign-on, and identity management.
Execution Framework	Infrastructure Manager, TOSCA templates	Deployment and orchestration of applications across heterogeneous infrastructures; supports multi-cloud and lifecycle management.
Persistent Identifiers	PID Service	Long-term identification and resolution of digital objects across the federation.
Monitoring	Monitoring Service	Collection and publication of availability and reliability metrics for EOSC Core and Exchange services.
Accounting	Accounting for Services; Accounting for Research Products	Usage tracking and aggregation of metrics for services and research outputs.
Helpdesk	Central Helpdesk and Adapters	Unified ticketing, support management, and integration with provider-specific helpdesks.
Messaging	ARGO Messaging Service	Reliable message exchange and notification system between federated components.
Resource Catalogue	Service Catalogue; Research Product Catalogue	Registration, discovery, and management of resources and providers within EOSC.
Order Management	Order Management System	Unified ordering and provisioning workflow across EOSC services.
Front Office	Explore; Discovery Hub; User Dashboard	User interface for researchers to discover, request, and access EOSC resources.

Table 1: EOSC Core Federating Capabilities

These federating capabilities form the cornerstone of the Sandbox architecture. They ensure that all Pilot EOSC Nodes and providers can integrate under a unified set of operational and interoperability principles, while preserving the autonomy and flexibility of their local deployments.

Another important requirement of the Sandbox is its usability and accessibility, which are equally essential for ensuring meaningful engagement within the EOSC Federation. The

Sandbox has therefore been implemented not only as a collection of interoperable services but also as an intuitive, structured environment where stakeholders can easily navigate, discover, and interact with the available tools.

The following section presents the Core Innovation Sandbox Home Page, which serves as the main entry point for all users, connecting them to the services, adapters, and documentation relevant to their specific role within the federation.

3.1. Core Innovation Sandbox Home Page

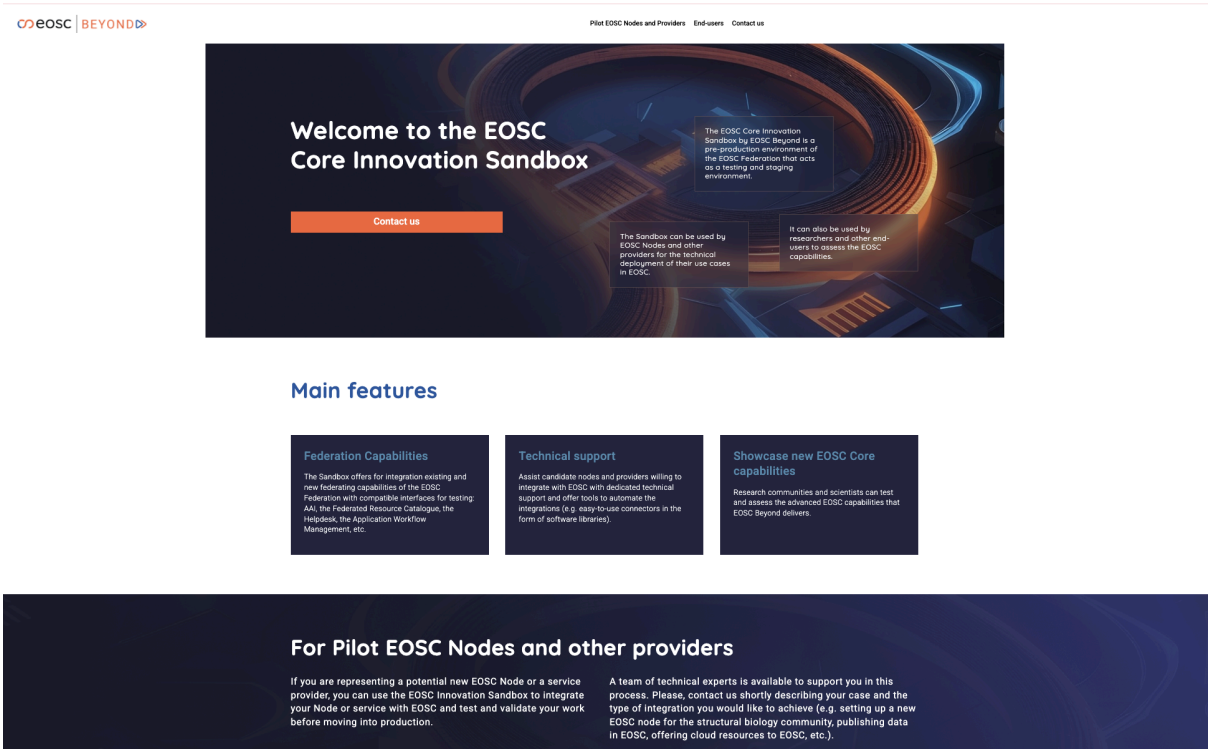

Figure 1: The EOSC Core Innovation Sandbox homepage

A central design choice was to introduce a dedicated landing page that immediately guides each stakeholder group —Core service providers, Exchange service providers, research communities, infrastructure operators, and developers— to the information and tools that are most relevant for them. This structure simplifies access and ensures that users can quickly identify the resources they need without navigating unnecessary complexity.

From this entry point, stakeholders are directed to their dedicated services, adapters, and the relevant sections of the EOSC Sandbox Documentation Hub. The integration of environment, services, and documentation is at the heart of the Sandbox architecture, ensuring that the Sandbox is not only a technical testbed but also a gateway into the EOSC Federation, supporting a seamless transition from experimentation to production readiness.

Beyond its design as a user-friendly entry point, the Sandbox homepage also reflects the structure of the environment itself. Each stakeholder group is guided not only to its relevant tools and services, but also toward the corresponding access pathways and onboarding

procedures. The following section describes these access models and engagement mechanisms, outlining how the main stakeholder groups interact with the Sandbox, gain access to its functionalities, and participate in the EOSC Federation testing process.

3.2. Access Models and User Engagement

The Sandbox engages a wide range of stakeholders, as described in Section 2.3, including Core and Exchange service providers, research communities, infrastructure operators, developers, and EOSC governance bodies.

However, this section focuses specifically on the three stakeholder categories that directly interact with the Sandbox environment through formal access and onboarding procedures — service providers, research communities, and infrastructure operators (Pilot Nodes) — which represent the main operational users of the platform. Access is therefore structured and role-aware, ensuring that all interactions are both effective and aligned with EOSC's standards.

- Service providers use the Sandbox to validate datasets, computational resources, and research services before onboarding them into a Pilot EOSC Node.
- Research communities test workflows, FAIR data practices, and reproducibility in a controlled setting.
- Infrastructure operators (current or prospective Pilot EOSC Nodes) validate interoperability, deployment strategies, and federated AAI integration prior to production.

Access to the Sandbox can be requested through the EOSC Beyond contact form, specifying the use case, technical needs, and support requirements. After that, the EOSC Beyond support team will guide the requestor according to its role and requirements. Details of the access procedures for the three roles follow.

3.2.1. Service Providers

For providers wishing to onboard resources in the Sandbox, the following additional requirements apply:

- **Legal Accountability** - The service provider must either be a legal entity or be connected to one (called the hosting legal entity), which takes full legal responsibility for the onboarded services or resources. If a service provider organization is not a legal entity, the hosting legal entity needs to be onboarded as an EOSC provider first.
- **Federated or Joint Resources** - When a resource is supplied by multiple organizations, the lead or coordinating provider handles onboarding. Additional contributors must also be registered as EOSC Providers and included as supporting providers in the resource profile.
- **Target EOSC Services or Communities** - Resources should be designed for EOSC users or communities, or based on EOSC Core capabilities. Additionally, services aimed at other communities can be onboarded if they utilize the EOSC infrastructure.

- **Effective Service Delivery** - Service providers need to ensure their services or resources are delivered reliably and effectively, including those provided by their collaborators.
- **Accurate and Up-to-date Information in English** - The service provider must ensure that all resource information is accurate and up-to-date by regularly updating contact details, links, and service statuses, and removing resources that are no longer available.
- **Support in English** - Services should provide at least basic support in English, covering user interfaces, documentation, instructions, and helpdesk assistance.

Generally, the onboarding process in the Sandbox ensures that only high-quality, interoperable resources are added to the Sandbox Catalogue, making them valuable to researchers. Since the sandbox is a testing environment, we strive to keep this process as simple as possible. Once a service provider registers, they can directly add their own resources—such as services, data sources, research products, or training materials—to the sandbox catalogue. The provider is responsible for registering and describing each resource they offer. To complete onboarding, the provider must provide information about their organization and each resource they want to include. This information must follow the EOSC profiles and are incorporated into the catalogue.

3.2.2. Research Communities

After authentication and registration in the Sandbox, research communities can navigate over the federated catalogue of the sandbox and freely request access to services and other capabilities offered for testing aims.

3.2.3. Infrastructure Operators - EOSC Pilot Node Deployment

Deploying a PilotEOSC Node begins with a thematic or national infrastructure provider deciding to connect its services and resources to the wider EOSC ecosystem. These resources may include compute, storage, data repositories, or domain-specific services. The first step is mapping the local Core capabilities to the EOSC Core federating services - particularly authentication and authorization, persistent identifiers, cataloguing, monitoring, and user support. This mapping ensures that once deployed, the Pilot Node is technically aligned with EOSC standards and compliant with its rules of participation.

Before a node can go live, providers are encouraged to deploy their setup within the EOSC Core Innovation Sandbox. The sandbox is organized into multiple stages (development, integration, and pre-production), allowing gradual refinement. This pathway reduces the risk of errors in production and provides access to EOSC Beyond technical experts for troubleshooting and onboarding support. Node operators can reuse and customise Sandbox components to implement Node functions.

After the node shows compliance and interoperability in the sandbox, it can start its operations as Pilot Node jointly supporting use cases with other Pilot Nodes. Operators can define and handle their custom onboarding procedures, and implement stricter governance

through service-level agreements to maintain reliability and transparency. Additionally, node operators should supply documented access policies for their resources, support helpdesk functions, and uphold FAIR data principles.

Deployment is not a one-off process but a continuous integration pathway. After going live, EOSC Pilot Nodes are expected to keep pace with evolving EOSC Core capabilities, new interoperability requirements, and updates in federated AAI or monitoring systems.

The project has established a maturity scale for Pilot Nodes, which varies depending on the core services they can adopt or develop within the federation. At a lower maturity level, a Pilot Node should at least integrate AAI (Authentication and Authorization Infrastructure) and a Catalogue service, which are essential for ensuring interoperability and resource discoverability within EOSC.

As the node advances in its maturity, it should evaluate and incorporate additional federating capabilities, such as Helpdesk, Monitoring, Accounting, and Messaging services, aligning its infrastructure with the EOSC Federation model. The aim is to attain the requisite level of readiness to be recognized as an EOSC Candidate Node, capable of contributing effectively to the federation's ecosystem.

3.3. Sandbox documentation hub

The Sandbox documentation hub is the central, practical guide for engaging with the technical infrastructure of the EOSC as enhanced by the EOSC Beyond project. This documentation hub serves as a hands-on resource for the key actors who build, contribute to, and use this federated network.

The site is organised to offer clear navigation paths for each audience:

- *Getting Started Guides* introducing first steps for participation;
- *Technical References* detailing APIs and service configurations;
- *Procedural Guides* for onboarding, registering resources, or configuring Pilot Nodes;
- *Support and Training Resources* with tutorials, materials, and helpdesk contacts.

As already mentioned earlier, each stakeholder group is redirected to a tailored section specific for its needs.

Built as an open, collaborative platform, the documentation content is maintained on GitHub (eosc-beyond-sandbox/eosc-sandbox) and published via **EOSC Documentation Hub**, ensuring transparency, version control, and community contribution. This model turns the documentation into a “living” resource that evolves with the project and reflects the principles of Open Science.

For EOSC Pilot Nodes

This section of the documentation acts as an operational handbook for organizations that want to become a foundational part of the federated EOSC.

It contains:

- Enrolling Procedures: A detailed checklist and guide on the technical and administrative requirements to be recognized as an official EOSC Pilot Node.
- Configuration Manuals: Instructions on how to configure a Pilot Node's local infrastructure to interoperate with the central EOSC Core services, covering aspects like authentication, monitoring, and resource reporting.
- Management Best Practices: Guidance on the day-to-day operation of a Pilot Node to ensure reliability and compliance with the federation's policies.

For Service Providers

For those looking to onboard resources into the EOSC Sandbox Catalogue and Front Office. It provides:

- Service Onboarding Guide: A step-by-step walkthrough of the process for describing a service, defining its access policies, and publishing it to the EOSC Sandbox Catalogue.
- Resource Management Instructions: Information on how to update service descriptions, manage user access, and view usage statistics.
- Integration with Core Services: Documentation explaining how to connect a service with essential EOSC functions like the central helpdesk and accounting systems.

For Developers and Integrators

This is the most technical section of the documentation, providing the necessary details for building applications and creating seamless workflows. Key resources include:

- The EOSC Integration Suite: A comprehensive guide to the portfolio of "software adapters" that enable interoperability. This is a critical resource for developers, with detailed documentation on how to use various adapters for catalogs, accounting, persistent identifiers (PIDs), messaging, and monitoring.
- API Reference: Detailed specifications for the REST APIs of the EOSC Execution Framework and other core services, including endpoints, parameters, and example code.

Reflecting the project's commitment to Open Science principles, the documentation is built using an open and collaborative model with modern, widely adopted tools.

- Content Repository on GitHub: The source content for the documentation is written in Markdown and hosted in the public eosc-beyond-sandbox/eosc-sandbox GitHub repository. The main branch, accessible at **link** allows anyone to view the content, suggest changes, or report issues directly. Using GitHub provides a powerful platform for version control and collaborative development.
- Presentation via GitHub Pages: The polished, user-friendly website at **https://docs.sandbox.eosc-beyond.eu** is generated and served using GitHub Pages. The site is built with MkDocs and the Material for MkDocs theme, providing a clean, navigable, and responsive user interface for accessing the documentation.

This open implementation strategy ensures the documentation is a "living document" that evolves with the EOSC Beyond project, incorporating feedback and contributions from the community it serves.

4. First integration report

At the time of reporting, all sandbox Core Federating Capabilities had been reviewed by the Pilot Nodes. The attached table shows the integrations each Pilot Node carried out. Some components were used as-a-service through the pre-production sandbox environment, while other Pilot Nodes opted to set up their own instances. This section explains how the Pilot Nodes interacted with and used the sandbox components, including specific deployment choices, interaction patterns, and performance observations.

	AAI	Execution Framework	Helpdesk	Monitoring	PID	Service Catalogue	Research Product Catalogue	User Space
CESSDA	DONE		DONE	DONE	IN PROGRESS	IN PROGRESS	IN PROGRESS	DONE
CNB-CSIC	IN PROGRESS	DONE						
e-INFRA CZ	DONE		DONE			DONE		
ENES	DONE	DONE	DONE	DONE		DONE		DONE
INSTRUCT-ERIC			DONE	DONE	DONE	IN PROGRESS		IN PROGRESS
LifeWatch ERIC	DONE	DONE	IN PROGRESS			IN PROGRESS		IN PROGRESS
METROFOOD-RI	DONE		DONE	IN PROGRESS		DONE		
NFDI	DONE		IN PROGRESS					IN PROGRESS
NI4OS-Europe	DONE		DONE			DONE	IN PROGRESS	IN PROGRESS

Figure 2: Overview of the sandbox components tested by pilot nodes

CESSDA successfully integrated several sandbox services, with AAI, Helpdesk, and Service Monitoring described as straightforward since the service owners didn't run into major issues during the integration process. The white label Front Office required significant technical expertise to configure and uncovered some bugs and missing features, but it provided useful functionality once deployed. Integration with the Service Catalogue, PID Service, and Research Product Catalogue is still underway, with early concerns around how best to adopt the PID service. Lessons learned highlight the ease of federating certain services, but also the need for more mature tools, clearer documentation, and streamlined onboarding across nodes.

CNB-CSIC's validation report service has been successfully deployed through the sandbox Deployment Service, using the Infrastructure Manager on multiple cloud sites, which demonstrates the reliability of containerized deployments. AAI integration is underway, with a proxy already set up, and connections to the Front Office and Order Management are planned next. The team aims to expand to integrating Helpdesk, Monitoring, and PID services in the next phase. Feedback indicates that while deployment is stable, the main challenge remains finalizing AAI interoperability to enable seamless user access and integration with the broader EOSC ecosystem.

For **e-INFRA CZ**, integrating AAI was a straightforward process due to their existing infrastructure, which already used sandbox-compatible technologies. Both the IaaS Cloud (OpenStack) and JupyterHub notebooks service are fully integrated with AAI. The Service Catalogue and Helpdesk are in use, although they're not yet deeply integrated, with plans to achieve machine-to-machine interoperability for the Helpdesk in the future. Overall, the feedback highlights the maturity of their technical environment and how easily it aligns with the sandbox services, while also noting their goals for tighter federation features.

ENES has successfully integrated with multiple sandbox services, including AAI, Helpdesk, Monitoring, Service Catalogue, Front Office, and Deployment Service. The AAI proxy allows for federated access across nodes, although it's only been tested in beta through EGI Check-in so far. Setting up Monitoring and Helpdesk was easy, requiring only a request for alerts on endpoint downtime. Service Catalogue and Front Office were efficient and well-synchronized, while Deployment using TOSCA templates needed some technical support but worked well overall. The ENES experience highlights the importance of coordinated support from sandbox components' owners, but also shows the need for production-ready AAI, clearer validation messages, and further refinement of templates and documentation.

At the time of reporting, **INSTRUCT-ERIC** was fully integrated with the Helpdesk, Front Office, and PID service. Its plans include adopting AAI for federated access and using storage brokering through ARIA and FandanGO to connect with external providers like EGI's OneData. This integration is a future development, but the design anticipates benefits from making structural biology data FAIR by linking raw data to researcher visits in ARIA and later publishing them via the resource catalogs.

LifeWatch ERIC has made solid progress in integrating sandbox services. Its Metadata Catalogue was successfully registered in the Sandbox Service Catalogue and federated as a data source, though the team noted the integration process could have been clearer and faster. The Deployment Service has been fully adopted, allowing automated provisioning of computational environments, though currently triggered from the command line rather than directly via the Front Office. AAI integration is complete and functional, enabling seamless authentication. The Helpdesk workflow has been tested successfully, allowing tickets to be routed to the LifeWatch technical team, but final refinements are still in progress. Future work includes completing integration with the Order Management System and enabling dataset harvesting into the Knowledge Graph.

The **METROFOOD-RI** pilot node has concentrated on connecting its services to a sandbox pre-production environment. Key steps included adopting AAI for federated authentication, adding services to the Service Catalogue, and getting them ready to be visible in the Front Office. Feedback highlighted challenges in aligning domain-specific metadata and making sure services are easy to find for users. Testing showed that the Monitoring and Helpdesk integration works, but more customization is needed to make the Helpdesk more relevant for METROFOOD's specific users. Deploying services through the sandbox was doable, but it took a lot of technical support to get workflows aligned with the TOSCA-based Deployment Service.

The **NFDI** pilot node successfully connected its own AARC-compliant AAI with the sandbox AAI, making the integration straightforward. Using the Front Office proved easy: services were registered in under an hour, and a sandbox Front Office was also deployed on a Kubernetes cluster for testing catalogue federation. Helpdesk integration is still in progress, as NFDI aims to have a dedicated tenant in the Sandbox helpdesk. Overall, feedback highlights that while AAI and Front Office adoption were smooth, further work is needed to refine helpdesk usage and to adapt the Front Office deployment to NFDI's distributed setup.

NI4OS-Europe AAI integration was completed successfully, allowing users to access services with their institutional credentials. The Service Catalogue and Front Office onboarding worked as expected, but feedback highlighted the need for clearer documentation and simpler service deployment. The Helpdesk system was tested and integrated, and monitoring integration is currently underway. Future plans aim to connect exchange services more closely with sandbox services, particularly to improve resource discovery and ensure consistent use of persistent identifiers (PIDs).

5. Conclusions and next steps

This document has introduced the EOSC Core Innovation Sandbox, a critical infrastructure component established by the EOSC Beyond project. The Sandbox is now operational, providing a robust and distributed pre-production environment designed to ensure the quality and seamless integration of services into the EOSC Federation.

The design, featuring Devel, Integration, and Pre-production instances, offers a structured pathway for providers to test, validate, and stage their resources. The access models and governance procedures detailed in this report have been established to create a clear and fair process for all stakeholders. As demonstrated in the first integration report, initial engagements with infrastructure operators and external providers have been successful, validating the Sandbox's architecture and its role as a vital testbed for the next generation of EOSC Core functionalities. The Sandbox effectively de-risks the integration process, fostering innovation and contributing to the overall stability and capability of the EOSC ecosystem.

The Sandbox is not only a technical environment but also a strategic enabler of the EOSC Federation, fully aligned with the objectives of the EOSC Beyond project. By lowering the barriers to experimentation, ensuring interoperability, and preparing nodes and services for production, it strengthens the federation model that lies at the heart of EOSC. Its role extends beyond the project lifetime: the Sandbox is expected to remain a permanent instrument supporting validation, onboarding, and innovation, thus contributing to the sustainability and scalability of EOSC in the years to come.

The successful launch of the Innovation Sandbox marks the beginning of a continuous effort to enhance the EOSC Federation. The immediate next steps will focus on expanding its use and refining its processes:

- **Automation of Integration**: further development and implementation of automated processes for service integration, leveraging EOSC Core adapters to streamline onboarding.
- **Expanded Access**: opening the Sandbox to a broader set of EOSC Exchange providers and external initiatives seeking to integrate with EOSC.
- **Pilot and EOSC Node Validation**: using the Sandbox as the main tool for deploying and validating the federation of EOSC Nodes in collaboration with project pilots.
- **Showcasing and Demonstration**: employing the pre-production environment to demonstrate new capabilities and provide tangible evidence of progress to the EOSC community.
- **Feedback and Refinement**: gathering structured feedback from Sandbox users to continuously improve access policies, documentation, and overall user experience.
- **Future Reporting**: updating the community on the growth of Sandbox usage, the number of providers involved, and the increasing complexity of onboarded services.

In conclusion, the EOSC Core Innovation Sandbox represents both a milestone of EOSC Beyond and a cornerstone for the future EOSC Federation. By combining technical

robustness with strategic value, it ensures that EOSC can grow as a stable, scalable, and innovative ecosystem that supports European Open Science.

Acronyms

Term	Definition
AAI	Authentication and Authorization Infrastructure
AMS	ARGO Messaging Service
API	Application Programming Interface
ARIA	Cloud platform for Access and Facility management
B2B	Business to Business
B2C	Business to Consumer
CESSDA	Consortium of European Social Science Data Archives
CERN	European Organization for Nuclear Research
CLARIN	Common Language Resources and Technology Infrastructure
CMCC	Euro-Mediterranean Center on Climate Change
CNB-CSIC	National Biotechnology Center | Spanish National Research Council
CYFRONET	Academic Computer Centre Cyfronet AGH
DARIAH	Digital Research Infrastructure for the Arts and Humanities
DOI	Digital Object Identifier
EB	EOSC Beyond
ENES	European Network for Earth System Modelling
ENVRI	Environmental Research Infrastructures
EOSC	European Open Science Cloud
ERIC	European Research Infrastructure Consortium
FAIR	Findable, Accessible, Interoperable, Reusable
GRNET	Greek Research and Technology Network
KIT	Karlsruhe Institute of Technology
LW	LifeWatch
METROFOOD-RI	Infrastructure for promoting Metrology in Food and Nutrition
NFDI	German National Research Data Infrastructure
NI4OS	National Initiatives for Open Science in Europe
OSCARs	Open Science Clusters' Action for Research and Society
PID	Persistent Identifier
RI	Research Infrastructure
SSHOC	Social Sciences and Humanities Open Cloud

SLA	Service Level Agreement
TCB	Technical Coordination Board
VRE	Virtual Research Environments
VR	Virtual Reality

Annex 1

A.1 Components and services

The core of the sandbox features a pre-production environment designed for testing essential EOSC services. Users can experiment with a broad range of these services, many of which are also deployable, allowing EOSC node operators to establish their own instances of these components and, consequently, deploy their own EOSC nodes. However, certain services — including Community AAI, Infrastructure Proxy, Accounting for Services, Monitoring Service, Research Product Catalogue, and Research Product Provider Dashboard — are exceptions to this deployment capability, remaining centrally managed rather than user-deployable.

A.1.1. AAI

The AAI component allows users to access all resources from the exchange layer (services and repositories) registered within the node using their own institute credentials (eduGAIN credentials). It also enables a single sign-on approach to be established not just within a single node but across all nodes in the EOSC Federation. The AAI component comprises three services: Core Infrastructure Proxy, Identity Hub, and Federated AAI Connector.

The **Core Infrastructure Proxy** is responsible for connecting core services, and it is composed of the following elements:

- The Service Proxy component, a multi-protocol service provider proxy, supports OAuth2, OpenID Connect, and SAML2 for connecting to services. It is connected to the Identity Proxy in the Identity Hub via OpenID Connect to authenticate users in a consistent way.
- The Access Management component is responsible for implementing policies based on entitlements and resource capabilities pertaining to the connected services. This information typically includes group membership and roles available via the Identity Hub and Infrastructure Proxy, for controlling access to the connected services.
- The Service Management component provides a web interface through which Service Owners of the EOSC Core Services can manage the lifecycle of their services.

The **Identity Hub** is a multi-protocol authentication proxy supporting OAuth2, OpenID Connect, and SAML2, responsible for user authentication and providing consistent user information to services in the EOSC Federated AAI. It is composed of the following elements:

- The Identity Proxy is a logical component that provides a consistent way for the EOSC Node services to authenticate users.
- The Service Proxy is the logical component responsible for connecting services.
- The Service Management component provides a web interface through which Service Owners of the connected services can manage the lifecycle of their services. This simplifies the registration and reconfiguration of services, minimizing operational and management efforts.

- The Account Registry is responsible for maintaining the user accounts, their attributes, and the user personal groups, ensuring that all users have the required attributes in the account profiles.
- Access Management is responsible for managing entitlements and resource capabilities pertaining to the connected services. This information typically includes group membership and roles retrieved by the Account Registry, for controlling access to the connected services.

The **Federated AAI Connector** is responsible for registering, maintaining, and publishing the trust anchors and the associated metadata for all the entities in EOSC Node, and provides common horizontal functionalities. It fetches, validates, and stores information about all connected services and identity providers.

A.1.2. Execution Framework

The primary purpose of the Execution Framework is to simplify the onboarding of deployable applications within EOSC and manage their operation on the underlying infrastructures. This component offers a **Deployment Service** to node operators, implemented via the Infrastructure Manager (IM). The IM is an open-source tool that deploys complex applications across multiple cloud back-ends like AWS and OpenStack. It handles virtual infrastructure provisioning, automated software deployment, and lifecycle management of these applications. Additionally, it supports the OASIS TOSCA standard for describing application architectures.

A.1.3 Helpdesk

The helpdesk component provides a centralized support and ticketing platform for users, service providers, and operators across the EOSC ecosystem. It ensures efficient handling of requests, incident reports, and service-related queries, while enabling transparent communication and monitoring of resolution progress. Integrated with other EOSC Beyond Core services, the Helpdesk plays a key role in guaranteeing a reliable user experience and operational continuity.

A.1.4 Messaging

The Messaging component handles the efficient communication between EOSC services. Currently, the component includes only one service - **Messaging Service**, which is built on the ARGO Messaging Service (AMS), an asynchronous messaging system based on open standards designed to be highly reliable and scalable. EOSC Messaging Service is essential in the EOSC ecosystem by bridging the gap in end-to-end interconnection between services, supporting technical interoperability, promoting the adoption of common standards, and serving as the main transport layer. The caching mechanism supported by the Messaging Service, with extended features for pull/push functionality, offers an easy solution for services that need to exchange information. With the AMS-library (a Python library) and AMS-UI, the service provides simple access to data without needing specialized knowledge about querying or interacting with the system.

A.1.5 Monitoring

The main goal of the Monitoring component is to collect and publish data about the availability and reliability of EOSC services. The component includes a single service - **Monitoring Service** - that offers insights into the availability and dependability of EOSC services across both the Core and Exchange layers. This service consists of two parts: the Core Monitoring Service, responsible for overseeing Core services, and the Exchange Monitoring Service, which manages Exchange services.

A.1.6 Accounting

The Accounting component collects and provides data on the use of specific services and repositories within an EOSC node. It is intended to encompass both services and research outputs, which is why this component includes two services: Accounting for Services and Accounting for Research Products.

The **Accounting for Services** platform is designed to simplify the collection, aggregation, and sharing of metrics across different infrastructures, providers, and projects. It features two key components: the Accounting User Interface, which serves as the main point of interaction for clients, providing a graphical interface to view and manage accounting data; and the Accounting API, a REST API that receives data from external systems, stores it in a database, and processes it to be easily accessible for queries via the user interface.

A.1.7 PID

The PID (Persistent Identifier) component manages the assignment and resolution of PIDs for providers and resources integrated into EOSC. The **PID Service** within this component provides a robust and reliable solution for the long-term identification and management of digital objects, underpinned by leading European data centers and cutting-edge technology. These are the main values of the PID Service:

- Global Persistence and Reliability: the PID Service ensures enduring identification of digital objects through a globally resolvable Handle System. This persistence is crucial for maintaining long-term access and usability of research data, tools, and resources.
- High Performance and Redundancy: Utilizing advanced data center infrastructure and a redundancy scheme compliant with ePIC Consortium's Quality of Service policies, the PID Service guarantees high performance and reliability. The primary-mirror federation architecture ensures that PIDs are mirrored across multiple providers, minimizing the risk of service disruption.
- Advanced Technology Integration: The service is based on B2HANDLE technology, incorporating the distributed Handle System solution for efficient storage, management, and resolution of PIDs. It supports both REST API and native Handle API, enabling seamless integration with middleware applications, end-user tools, and other services.
- Flexible and Accessible Interfaces: The PID Service provides both a REST API and a native Handle API, catering to diverse user needs. These interfaces facilitate easy

integration and interaction with the PID service, whether for managing data objects or integrating with other digital infrastructures.

- Secure and Scalable Infrastructure: Leveraging the latest advancements in virtualization and data storage technologies, the PID Service ensures secure, scalable, and efficient handling of PIDs. This infrastructure supports a wide range of applications, from catalogues and registries to training materials and guidelines.
- Global Resolve Capability: PIDs are globally resolvable through the DONA Global Handle Registry network, ensuring that identifiers remain consistent and accessible across different systems and locations, regardless of changes in object location or ownership.
- Comprehensive Coverage: The PID Service supports a broad spectrum of catalogues and registries, including services/providers, tools, training materials, and guidelines, enhancing the traceability and management of various digital resources.

By delivering a high-performance, reliable, and globally accessible PID service, the PID Service ensures that digital objects are effectively managed and identified over time, supporting the integrity and continuity of research and data management efforts.

A.1.8 Resource Catalogue

The resource catalog enables the EOSC node to share resources, making the EOSC node's exchange resources discoverable. It also facilitates the creation of the EOSC federation and provides a search engine that covers the entire EOSC Federation, along with interfaces that enable EOSC Nodes to publish and retrieve resources within the federated catalog. The component includes two services: Service Catalogue and Research Product Catalogue.

The **Service Catalogue** provides data and functionality to register, maintain, administer, and share resources onboarded by various providers. It also serves as the point of reference for all EOSC Core components that add value to this information, making the data and services searchable and accessible through various tools for both researchers and end users.

Service Catalogue has two main elements: Registry and Provider Dashboard.

The Registry offers the underlying storage functionality and the interoperability tools for the programmatic access, registration, and management (CRUD) of providers, services, and catalogs. It also offers the necessary API functionality for the interoperability of service catalogs from individual providers or aggregators (e.g., thematic or regional catalogs).

The Providers Dashboard facilitates front-end functionality for registering providers and organizations that are eligible to publish their resources in the catalog. It offers features for onboarding and managing these resources effectively. Additionally, the dashboard provides representatives from provider organizations with a comprehensive view of their offerings, along with various usage statistics related to their resources. Moreover, it supports members of the onboarding team by providing tools to manage entries, oversee the onboarding process of providers, and audit the resources that have been onboarded.

A.1.9 Order Management

The order management component provides a framework for providers to define their service offers and for end-users to request access to EOSC services. **Order Management Service** within this component is a set of tools, processes, and guidelines designed to facilitate a unified ordering process for resources, providing a uniform experience for users and enabling efficient resource management for providers. It provides a coherent user journey from resource discovery to procurement within the Front Office, enhancing the user experience and supporting inter-provider communications to improve resource composability and outreach. Furthermore, it integrates various Order Management Systems through a flexible API, allowing seamless communication between the Front Office and provider-specific Order Management Systems. This integration supports a wide range of provider use cases, enabling efficient resource provisioning and order management.

A.1.10 Front Office

The Front Office component is a platform where researchers can find, request, and access the services, analytical tools, data management tools, storage, and computing resources they need for their work. It is an integrated system that provides easy access to many services across different research fields, along with data and integrated data analytics tools. Additionally, the Front Office promotes services and resources from local, national, and international providers, such as European e-Infrastructures and Research Infrastructures, with the goal of increasing access for a wider international user group. The component includes the following services: Explore, Resource Discovery Hub, and User Dashboard.

Explore Service is a key part of the EOSC Beyond initiative, offering researchers an easy-to-use platform to find, access, and integrate a wide variety of scientific resources from multiple EOSC Nodes. Using the EOSC Interoperability Framework, the Explore Service guarantees seamless cross-domain access and adherence to FAIR data principles, enabling researchers to build scientific workflows, encourage collaboration, and speed up scientific discoveries within a federated Open Science ecosystem.

The **Resource Discovery Hub** offers a research-oriented tool that helps users effectively find, manage, and reuse a variety of resources within the EOSC ecosystem. Users can access highly relevant content tailored to their preferences through an intuitive interface and advanced filtering options, providing a successful research experience that fits their workflows and expectations.

The **User Dashboard** is an AI-powered, somewhat personalized environment that displays users' personal website spaces. Each user can create and customize their scientific profile and, based on it, receive resources tailored to their needs. The dashboard helps users find resources aligned with their specific fields of interest, making it easier to explore the EOSC Resource Discovery Hub. It features an informative landing page and a personal subpage accessible only to authenticated users.