Grant Agreement 101079792, RESILIENCE PPP

IT Services Catalogue

Title of Deliverable:	IT Services Catalogue		
Deliverable Number:	D2.3 - FINAL		
Type of Data:	Report		
Lead Beneficiary:	FSCIRE		
Publishing Status	Public		
Last Revision Date:	23/04/2026	**by:**	R. DEMO
Verification Date:	24/04/2026	**by:**	Board
Approval Date:	DD/MM/YYYY	**by:**	[Name]
Document Name:	RESILIENCE_WP2_D2.3_ITServicesCatalogue_01.02.docx		

Funded by
the European Union

Change History

Version Nr	Date	Status	Name	Summary of Main Changes
00.01	25/10/2024	DRAFT	Initial Draft	
00.02	04/11/2024	Final Draft	First Review	Comments from KULeuven
00.03	11/11/2024	Final Draft	First Review	Comments from KULeuven
01.00	12/11/2024	BETA Final	-	Release of the Beta version
01.01	27/03/2026	Draft FINAL	-	Release of the draft of the FINAL version
01.02	23/04/2026	FINAL	Final revision	Comments from RESILIENCE CEO and CTO

Table of Content

1 Introduction

1.1 Objectives of this document

1.1.1 From the proposal

Extract from R1: “D2.3: IT Services Catalogue: organised, curated and documented collection of any and all IT services supporting the user services operated on the RESILIENCE platform.”

1.1.2 Detailed objectives

The IT Services Catalogue aims to provide a comprehensive overview of the core technical services that form the backbone of the RESILIENCE Research Infrastructure (RI) in religious studies. These IT services are essential for enabling the delivery of user services to the scientific community, ensuring the performance, scalability, and robustness required to support large-scale, data-intensive research. They are critical for facilitating collaboration, data sharing, and computational activities among researchers in the field.

Aligned with the European Open Science Cloud (EOSC) initiative, these services offer researchers advanced tools while ensuring compliance with key principles such as Open Science, FAIR data principles, and GDPR. The catalogue details each service's functionality and its role in supporting the research lifecycle, meeting the technological needs of modern interdisciplinary research within religious studies.

This document presents services that are proven in real-world research environments, providing scalable solutions that align with the maturity and robustness required by large-scale infrastructures like RESILIENCE.

For clarity, the catalogue distinguishes between concrete operational services (see Section 3) available to RESILIENCE users, services accessed through trusted external providers, and supporting standards, guidelines, or implementation practices (see Section 4) that enable integration, security, and future service evolution. In this context, **RESILIENCE does not aim to duplicate generic IT services that are already mature and widely available through established e-infrastructure providers, but rather to make use of existing resources where possible and integrate them into the broader RESILIENCE service environment**.

Where an item is a planned capability for a later implementation phase rather than an operational service, this is stated explicitly in section 3.1. This applies in particular to internal enabling capabilities and to governance, security, or interoperability frameworks that may support future RESILIENCE service delivery, but which are not yet intended to function as operational end-user services.

This Deliverable "D2.3 IT Services Catalogue" is a strategic mapping and planning document that identifies the external IT services on which RESILIENCE can rely and outlines the technical and governance conditions required for future coordinated implementation of enabling IT capabilities. This catalogue is pivotal for documenting, analysing, and planning the IT services that will support the project's User Services in the field of religious studies research. Note that we do not claim that all headquarters-level IT capabilities described in it will be operational in the near term. Where

mature third-party services already exist, RESILIENCE can map and rely on them already during the current preparatory trajectory. By contrast, internal enabling capabilities, governance mechanisms, and supporting policy frameworks are mainly design and planning elements for later implementation phases.

Accordingly, this document combines:

i. a mapping of external IT services that can support RESILIENCE user services; and
ii. an outline of the standards, requirements, and internal capabilities that would be needed for future coordinated implementation and operation.

1.1.3 Scope of D2.3 and relation to D2.2

This deliverable should be read together with D2.2 User Services Catalogue. D2.2 focuses on the services visible to researchers and on the onboarding of in-kind and community service contributions. The present deliverable complements D2.2 by documenting the IT layer that enables such services.

For clarity, the overall RESILIENCE service landscape can be understood as comprising three categories of user-facing services:

i. **core services** that may in the future be centrally managed by RESILIENCE headquarters;
ii. **community services** contributed by national nodes, partners, or the wider RESILIENCE community; and
iii. **third-party IT services** such as compute, storage, notebook environments, large file transfer, virtual machines, and related infrastructure offered by specialised e-infrastructure providers.

The present deliverable focuses primarily on the third category. These are mature, non-domain-specific IT services already offered by specialised providers such as EOSC-related infrastructures and e-infrastructures. RESILIENCE can therefore rely on them to support its user services without duplicating generic infrastructure capacity that is not specific to Religious Studies.

In addition, some technical capabilities may in the future exist at headquarters level to support federation, hosting, authentication, and operational coordination across the RESILIENCE ecosystem. These internal capabilities are not end-user services and are therefore not presented here as catalogue entries for researchers.

Likewise, the security, interoperability, onboarding, and software-development elements discussed in this document should be understood as enabling frameworks and requirements for future implementation rather than as stand-alone end-user services.

1.1.4 Long-term objectives

The IT services in this catalogue are designed around the following principles:

- **User-Centric Design**: Services are tailored to meet the specific needs of researchers in religious studies, ensuring ease of use, high performance, and flexibility.

- **Sustainability, Scalability, and Security**: Services are built to grow with increasing research needs, ensuring long-term sustainability through secure and scalable access and functionality.
- **Compliance with Open Science and Research Policies**: Services comply with **Open Science**, **FAIR data principles**, and **GDPR**, supporting transparency, reproducibility, and long-term accessibility of research outputs.
- **Maturity and Robustness**: The IT services demonstrate high **Technology Readiness Levels (TRL 8-9)** to ensure reliability. They integrate with the broader research ecosystem, enabling seamless collaboration and access to computational, storage, and network resources.
- **Alignment with EU Green ICT Objectives**: In line with the EU's commitment to green digital transformation, the IT services prioritize energy efficiency, sustainable data management, and eco-friendly practices. This includes promoting energy-efficient digital infrastructures, exploring low-power computing solutions, and supporting sustainable practices across data centers and cloud services.

2 Operational IT Services

2.1 Access to Physical & e-Infrastructures

This section covers services enabling access to essential physical and electronic infrastructures. RESILIENCE leverages existing resources like **CINECA**, **EURO HPC** and **EOSC EU Node** to avoid the need for purchasing physical hardware. This approach ensures scalability and flexibility while aligning with modern scientific standards such as Open Science and FAIR data.

2.1.1 Compute Resources

Services offering computational resources for processing large datasets and complex computations required in research projects.

- **Access to HPC and Cloud Resources**: Through partnerships with **CINECA**, **EGI**, **EURO HPC and EOSC EU Node**, researchers gain access to high-performance computing (HPC) and cloud-based computing resources.
    - **CINECA**: Through ISCRA, CINECA provides access to a broad portfolio of advanced computing resources, including the LEONARDO Tier-0 EuroHPC supercomputer, the GALILEO100 Tier-1 system, Big Data resources, public Cloud infrastructure, and quantum computing resources. For more interactive workflows, CINECA also offers a browser-based JupyterLab environment on Galileo100, enabling near-immediate access to GPU-equipped nodes for exploratory and iterative analysis.
    - **EuroHPC JU**: EuroHPC provides access to European supercomputing resources through a single MyEuroHPC entry point. Its EuroHPC Federation Platform federates computational and data-analysis capabilities, advanced software environments, and high-performance storage across hosting entities. Access is supported through secure MyAccessID login and through a web-based Open OnDemand interface, making EuroHPC resources easier to reach and combine across Europe.
    - **EOSC EU Node**: The EOSC EU Node offers researchers access, via institutional credentials, to virtual machines, GPU resources, interactive notebooks, containerised workflows, storage, data transfer, and collaborative tools within its User Space. Its compute services include OpenStack CPU/GPU clusters, on-demand customisable virtual machines, Jupyter-based Interactive Notebooks, and a Cloud Container Platform based on simplified Kubernetes. This makes the EOSC EU Node relevant both for exploratory work and for scalable, reproducible execution environments.

2.1.2 Data Storage Solutions

The services listed in this section were selected as representative examples rather than as an exhaustive inventory. Their inclusion was guided by a combination of criteria: relevance to the core technical needs of RESILIENCE user services, maturity and operational reliability, alignment with Open Science, FAIR, and GDPR-related requirements, integration potential within the wider European research ecosystem, and their ability to provide scalable, reusable, and non-domain-specific infrastructure without duplicating existing e-infrastructure capacity. Attention was given to services that support key functions such as compute, storage, data transfer, persistent identification, secure collaboration, reproducibility, and interoperability, and that are already offered by trusted providers with established governance and support structures.

Services providing scalable and secure storage for large datasets and research outputs.

- **RESILIENCE Community (Zenodo Community)**: A dedicated Zenodo community can function as the curated RESILIENCE space for deliverables and research outputs. Zenodo communities allow projects, institutions, and domains to manage members, review submissions, and curate content in a shared environment. Where appropriate, an EU Project Community also ensures visibility in the EU Open Research Repository and applies automated curation checks aligned with Horizon Europe open science requirements. All deliverables respecting our D2.4 Data Management Plan, in which the metadata requirements are included, are published as part of our community.
- **Zenodo Integration**: Zenodo supports long-term publication and citation of research outputs by assigning a DOI to every upload, making records immediately citable and trackable. It also supports versioning, so updated datasets or outputs can remain separately citable while preserving earlier versions. In addition, Zenodo offers collaboration and sharing features through communities, user sharing, secret links, and access requests for restricted or embargoed content.
- **EUDAT – B2SHARE**: B2SHARE is a user-friendly service for storing, preserving, and publishing research data. It supports persistent identifiers, user-defined access policies, community-specific metadata extensions, openly harvestable metadata, metadata versioning and management, and API-based integration with community workflows. The service is professionally managed, includes backup and disaster-recovery arrangements, and is integrated with other EUDAT services such as B2ACCESS, B2FIND, and B2HANDLE.
- **EUDAT – B2DROP**: B2DROP is a secure synchronisation and sharing environment for active research data. It supports multiple file versions, desktop synchronisation, WebDAV access, sharing across B2DROP and ownCloud/Nextcloud instances, and onward publication of datasets to B2SHARE. This makes it particularly suitable for collaborative workspaces where files need to remain synchronised and shareable during the research process.
- **EOSC EU Node**: For storage and data movement, the EOSC EU Node offers File Sync-and-Share for collaborative versioned cloud storage, Large File Transfer for encrypted exchange of large datasets, and Bulk Data Transfer for moving massive research data volumes quickly and reliably. These services are integrated into the User Space virtual research environment, where projects, teams, data, and services can be managed from a single dashboard.
- **D4Science – StorageHub**: StorageHub provides centralised storage with robust access controls and encryption, combined with file versioning, history management, backup, metadata management, and data organisation. Within the broader D4Science Data Storage Framework, it is integrated with Workspace, Accounting, Data Sovereignty, federated identity, and VRE services. This enables secure storage and reuse of data across D4Science tools and applications, including environments such as JupyterLab, RStudio, and CCP.

2.1.3 Virtualization

Virtualization services provide flexible, isolated environments for conducting research experiments, developing software, and managing computational workflows. By using virtual machines (VMs) or containerized applications, researchers can create customizable, reproducible setups for their projects without needing dedicated physical hardware. This approach enables efficient use of resources, scalability, and easy deployment across various platforms.

- **Virtual Machines (VMs)**: Through partnerships with providers like EOSC EU Node, CINECA, D4Science and EGI, RESILIENCE offers access to virtual machine resources, allowing researchers to configure isolated computing environments tailored to their specific needs.
- **The Interactive Notebooks service** on EOSC EU Node is a managed JupyterHub environment that allows researchers to create and share documents with live code, equations, and visualizations
- **Containerized Environments**: Utilizing container platforms (e.g., Kubernetes (OKD distribution) on EOSC EU Node), researchers can deploy and manage applications with increased portability, ensuring consistent performance and reproducibility across different infrastructures.

2.2 Security & Operations

The Security & Operations services are foundational to maintaining the integrity, reliability, and resilience of the research infrastructure. This section covers critical IT services dedicated to safeguarding data, managing secure access, and ensuring the smooth, uninterrupted operation of IT resources. By implementing robust security measures and comprehensive infrastructure management practices, these services support the trustworthiness and sustainability of the research ecosystem.

The Security & Identity Management services focus on protecting sensitive information and controlling access through reliable authentication and encryption methods. Meanwhile, Operations & Infrastructure Management services are responsible for monitoring and maintaining system performance, automating key functions, and preparing for disaster recovery to support ongoing research activities.

Together, these services provide a secure, stable, and efficient operational environment that aligns with compliance standards and best practices, ensuring researchers can rely on an infrastructure that meets high standards of security and reliability.

To these objectives, RESILIENCE has published D2.7 - Security Management Plan a comprehensive document that encompasses all the aspects of the entire project's security landscape.

2.2.1 Security & Identity Management

Services dedicated to protecting the infrastructure, securing user access, and managing user identities.

- **Authentication & Authorization Infrastructure (AAI)**: Implements secure login mechanisms such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) using platforms like **My Access ID**, **eduGAIN** and **EGI Check-in**.
- **Data Encryption**: Ensures data is encrypted both in transit and at rest to protect sensitive information.
- **Security Monitoring & Incident Response**: Provides continuous monitoring for security threats and a defined response plan for incidents.

2.2.2 Operations & Infrastructure Management

Services ensuring reliable infrastructure performance and maintenance.

- **Monitoring & Alerting Systems**: Implements real-time system performance and uptime monitoring using tools like **Nagios** or **Zabbix**.
- **Automation & Orchestration**: Utilizes automation tools for backups, load balancing, and service scaling with technologies like **Ansible** and **Kubernetes**.
- **Disaster Recovery & Business Continuity**: Establishes backup services to ensure minimal downtime and data loss, maintaining continuity of research activities.

3 Supporting standards, guidelines, or implementation practices

This section groups the cross-cutting standards, policy references, architectural principles, and implementation practices that underpin the operational IT services described above. Unlike the services themselves, these elements function as enabling mechanisms for interoperability, security, reproducibility, maintainability, and future service evolution across the RESILIENCE Research Infrastructure.

3.1 Future Implementation Framework

This section groups the technical, organizational, and policy elements that support secure and interoperable service provision across RESILIENCE. Unlike the operational IT services listed above, these elements are not catalogue entries intended for direct use by researchers. Instead, they define the enabling conditions for future federation, governance, integration, security, and service evolution.

(i) Internal headquarters-level enabling capabilities

In later implementation phases, RESILIENCE may require a limited set of centrally coordinated technical capabilities at headquarters level. These may include hosting support for centrally managed core services, federation and Authentication and Authorization Infrastructure support for community services, and shared operational coordination functions such as monitoring, service integration, and platform-level management.

Such capabilities are internal enablers for the RESILIENCE federation of resources. They are not intended as end-user services in the RESILIENCE service catalogue, even if they may support national nodes or service owners in connecting their services to the wider RESILIENCE environment.

(ii) Supporting standards and implementation guidelines

The future RESILIENCE IT environment will rely on a set of cross-cutting standards and implementation practices, including alignment with Open Science and FAIR principles, GDPR compliance, secure authentication and authorization, encryption, monitoring and incident response, standardized APIs, data interoperability standards, middleware solutions, version control, CI/CD, testing, and documentation.

These elements should be understood as guiding requirements for secure integration and maintainable service delivery. They define how services should interoperate, how risks should be managed, and how future technical implementation should remain robust and sustainable.

(iii) Service onboarding and future evolution

The onboarding and evolution of future services will require structured procedures, alignment with RESILIENCE strategic objectives and technical standards, and regular review based on user feedback and technological developments. Where services are to become operational within the RESILIENCE environment, a high level of maturity will be expected.

The following subsections therefore can represent a framework for future implementation, continuous improvement, and federation readiness rather than a set of operational services already in place.

3.2 Cross-cutting Standards and Policy Alignment

The following cross-cutting references guide the design, integration, and operation of RESILIENCE services:

- **Open Science and FAIR Data Principles**: RESILIENCE services are designed to align with Open Science practices and FAIR data principles to support transparency, interoperability, and long-term reuse of research outputs.
- **D2.4 Data Management Plan**: The D2.4 Data Management Plan provides the reference framework for metadata requirements, data interoperability, and compliance with Open Science recommendations.
- **GDPR Compliance**: All relevant services and implementation practices are expected to respect GDPR requirements and related data protection obligations.
- **D2.7 Security Management Plan**: The D2.7 Security Management Plan provides the overarching framework for security governance, secure access, data protection, incident response, and operational resilience.
- **D2.8 Software Development Plan**: The D2.8 Software Development Plan provides guidance on software development, testing, documentation, version control, release management, and long-term maintenance.

3.3 Security and Operational Good Practices

The secure and reliable operation of RESILIENCE services is supported by a common set of security and infrastructure management practices, including:

- **Authentication and Authorization Infrastructure (AAI)**: Secure user authentication and authorization mechanisms support controlled access to services and data.
- **Single Sign-On (SSO) and Multi-Factor Authentication (MFA)**: These mechanisms strengthen identity management and reduce unauthorized access risks.
- **Data Encryption**: Data should be protected both in transit and at rest through appropriate encryption measures.
- **Security Monitoring and Incident Response**: Continuous monitoring and defined incident response procedures support timely detection and mitigation of threats.
- **Monitoring and Alerting Systems**: Real-time performance and availability monitoring help ensure service reliability.
- **Automation and Orchestration**: Automation tools support operational efficiency in areas such as backups, load balancing, and service scaling.

- **Disaster Recovery and Business Continuity**: Backup and recovery mechanisms help minimize downtime and preserve continuity of research activities.

3.4 Integration and Interoperability Practices

The Service Integration and Interoperability section addresses the technical frameworks and best practices needed to connect and align RESILIENCE infrastructure with other research platforms. Ensuring seamless integration and data interoperability is essential for fostering collaboration, expanding resource access, and aligning with the broader European Open Science ecosystem, including platforms like EOSC and SSHOC Open Marketplace.

Service integration focuses on establishing standard APIs, data formats, and middleware solutions that enable RESILIENCE to interact smoothly with other research infrastructures. These efforts support the flexible exchange of data and applications, adhering to Open Science and FAIR principles. In addition, Recommendations for Developers provide essential guidelines for researchers and developers to design systems that are interoperable, secure, and compliant with key standards. By adopting open standards, prioritizing security, using modular architecture, and maintaining rigorous testing and documentation, developers can ensure that their systems can integrate seamlessly with the RESILIENCE infrastructure, enhancing both the robustness and accessibility of research services.

To support effective interaction with external infrastructures and platforms, RESILIENCE promotes the following integration and interoperability practices:

- **Standardized APIs**: Standard APIs support integration with external environments such as EOSC, SSHOC Open Marketplace, and other relevant research infrastructures.
- **Data Interoperability Standards**: Shared data formats and metadata practices improve exchange, reuse, and interoperability of research data.
- **Middleware Solutions**: Middleware supports cross-platform data exchange and service integration.
- **Service Registries**: Registries help catalogue and discover available services within the RESILIENCE ecosystem.
- **Interoperability Layers**: These layers facilitate technical integration between heterogeneous platforms and services.
- **Data Mapping and Transformation Tools**: These tools support the alignment of data originating from different systems through common standards and ontologies.
- **Metadata Harvesting Services**: Harvesting mechanisms improve discoverability and support FAIR compliance across platforms.
- **API Management Platforms**: These support the secure exposure, governance, and maintenance of APIs for research services.

3.5 Recommendations for Developers

To ensure that systems deployed on RESILIENCE RI are interoperable, secure, and maintainable, developers should follow these recommendations:

1. **Adopt Open Standards**: Use open standards such as RESTful APIs and OAuth2 to support seamless integration.
2. **Security by Design**: Implement encryption, secure authentication, and GDPR-aware practices from the outset.
3. **Modular Architecture with Containerization**: Use modular design principles together with container technologies such as Docker and Kubernetes to support portability, scalability, and maintainability.
4. **Compliance with FAIR and Open Science**: Ensure that systems align with FAIR principles and support Open Science practices.
5. **Testing and Documentation**: Provide sufficient testing, technical documentation, and user documentation to support reliable integration, operation, and maintenance.

3.6 Implementation Practices for Reproducibility, Onboarding, and Future Evolution

The Service Onboarding and Evolution section outlines the preliminary framework for incorporating new IT services into the RESILIENCE infrastructure while ensuring they remain relevant and aligned with evolving research needs. The detailed processes, standards, and tools for onboarding and service evolution will be defined in upcoming phases of the project, particularly during the implementation phase. This approach is crucial for maintaining a flexible and scalable research environment that can adapt to emerging technologies and user requirements.

Detailed onboarding procedures are not part of the current PPP and will instead be specified in the next phase of RESILIENCE, in line with the IT work foreseen in TIP. Building on the D2.4 Data Management Plan and D2.7 Security Management Plan, that work will finalize the design of a modular RESILIENCE IT architecture and the associated governance framework, including the roles, expertise, responsibilities, and policy frameworks needed for coordinated IT and service management at RESILIENCE headquarters and across its service environment. Within that future framework, onboarding procedures will provide a structured approach for evaluating and integrating new services, with particular attention to interoperability, security, data protection, and alignment with FAIR principles and European frameworks. Services intended for full operational onboarding are expected to reach a Technology Readiness Level (TRL) of 9, ensuring that they are fully operational, reliable, and robust for use by the research community.

Continuous Improvement and Roadmap planning will be conducted during the implementation phase. This process will involve regular assessments and updates based on user feedback and technological advancements. By planning these activities for the implementation phase, RESILIENCE ensures that it can offer state-of-the-art tools and platforms that meet the highest standards for performance and interoperability.

The following subsections outline services that facilitate integration at multiple levels: Aggregators & Integrators for combining various research platforms, Data Aggregation to ensure interoperability

of research data, Application and Software Integration to support flexible deployment and collaboration, and Additional Support Services that provide training and technical support for seamless use and adoption.

Some of these services are planned for future development, while others involve leveraging existing tools from RESILIENCE or other providers. These efforts collectively aim to enhance the research capabilities within RESILIENCE, creating a cohesive ecosystem where services, data, and applications work in concert to support the academic community.

Beyond operational services, RESILIENCE also relies on implementation practices that support reproducibility, scalability, and long-term service evolution, including:

- **Virtualization**: Virtual machines provide isolated and configurable environments for research workflows and software deployment.
- **Interactive Notebooks**: Managed notebook environments support reproducible research workflows and facilitate exploratory analysis.
- **Containerized Environments**: Container-based deployment improves portability, consistency, and reproducibility across infrastructures.
- **Version Control Systems**: Platforms such as GitHub or GitLab support collaborative software development and controlled evolution of code and documentation.
- **Continuous Integration / Continuous Deployment (CI/CD)**: Automated pipelines support software quality, controlled release processes, and reliable deployment practices.
- **Onboarding Procedures**: New services should be evaluated through structured onboarding procedures aligned with RESILIENCE strategic objectives and technical standards.
- **Technology Readiness Level (TRL)**: Operational services are expected to demonstrate a high level of maturity, with TRL 9 as the target for fully onboarded services.
- **Continuous Improvement and Roadmap Planning**: Services should evolve through regular assessment, user feedback, and adaptation to technological developments.
- **Training and Documentation**: Clear documentation and training materials are essential for effective service adoption and integration.
- **Technical Support and Consultancy**: Expert support helps research teams integrate their services, data, and applications with the RESILIENCE platform.

This section provides the non-service foundations that make the RESILIENCE service ecosystem secure, interoperable, scalable, and sustainable over time.

3.6.1 Aggregators & Integrators

3.6.1.1 Service Aggregation

This section introduces services and tools that integrate various platforms, tools, and data sources, enhancing research capabilities within the RESILIENCE infrastructure. These are guidelines and principles that will inform the development and integration of services in later project phases. The

focus is on ensuring that the RESILIENCE infrastructure can effectively interoperate with other research platforms and resources.

Services that aggregate research tools and services into a unified platform:

- **Service Registries**: Tools for cataloguing and discovering available services within the RESILIENCE ecosystem.
- **Interoperability Layers**: Middleware facilitating integration between different research platforms.
- **Service Monitoring Dashboards**: Tools for tracking service health and availability across infrastructures.

3.6.1.2 Data Aggregation

Support for data integration and interoperability:

- **Data Mapping and Transformation Tools**: Allow researchers to integrate and align data from different sources using common standards and ontologies.
- **Metadata Harvesting Services**: Tools for collecting metadata across platforms to ensure FAIR compliance and enhance discoverability.

3.6.1.3 Application Integration

Integration of research applications with existing services:

- **API Management Platforms**: Tools to securely expose and manage APIs for research services.
- **Containerization and Virtualization**: Use of containerized environments for easy deployment and scaling of research applications across infrastructures. See also section 3.1.4.

3.6.2 Software Integration

Support for software development and integration:

- **Version Control Systems**: Encourages the use of platforms like **GitHub** or **GitLab** for managing software projects and collaborations.
- **Continuous Integration/Continuous Deployment (CI/CD)**: Integrates automated testing and deployment pipelines to ensure software reliability.

For more information, consult D2.7 section 7.1 (Secure Software Development Lifecycle + DevSecOps) and/or the D2.8 Software Development Plan.

3.6.3 Additional Support Services

Other integrative services for researchers:

- **Training & Documentation**: Provides comprehensive documentation and training materials for researchers to effectively use and integrate services.
- **Technical Support & Consultancy**: Offers expert assistance to help research teams integrate their services and data with the RESILIENCE platform.

4 Conclusion

This deliverable should be understood as a mapping and structuring document for the IT layer that supports RESILIENCE user services. It identifies mature third-party e-infrastructure services that RESILIENCE can rely on for compute, storage, virtualization, notebook environments, and related capabilities, and it outlines the internal enabling capabilities and policy frameworks that will be needed for future coordinated IT management.

In this sense, D2.3 complements rather than duplicates D2.2. The User Services Catalogue focuses on the services visible to researchers and on the onboarding of community contributions, while the present document clarifies the external IT resources, technical standards, and future governance conditions required to sustain that service landscape.

Except where mature third-party services are already available and can be relied upon, the headquarters-level enabling capabilities described here remain part of the design and planning work for later implementation phases rather than fully operational services for the next project year.

5 Annexes

5.1 Glossary of Terms

Term	Definition
API (Application Programming Interface)	A set of protocols that allow different software systems to communicate with each other, essential for integrating services in RESILIENCE with external platforms.
Authentication & Authorization Infrastructure (AAI)	Systems that manage user identities and control access to resources, using secure login mechanisms like SSO and MFA.
CESSDA	The Consortium of European Social Science Data Archives, which offers tools, data, and training specifically for social sciences research.
Compliance with Open Science and Research Policies	Ensures alignment with Open Science, FAIR data principles, and GDPR to support transparency, reproducibility, and accessibility of research outputs.
CI/CD	Continuous Integration/Continuous Deployment: Automated software development processes that include regular testing and deployment, ensuring reliable and consistent software updates.
DARIAH	A European Research Infrastructure Consortium for the arts and humanities that provides digital tools and resources for research in these fields.
Data Interoperability Standards	Standards that ensure data from different sources can be combined and used together, supporting seamless data exchange and integration.
Disaster Recovery & Business Continuity	Systems and protocols that ensure service and data recovery in the event of a system failure or disaster, ensuring research continuity.
European Open Science Cloud (EOSC)	A European initiative providing a cloud-based environment that enables researchers to store, share, and analyze data, supporting Open Science practices across disciplines.
FAIR Principles	Guidelines to ensure that data is Findable, Accessible, Interoperable, and Reusable, supporting open data standards and interoperability in research.
GDPR	The General Data Protection Regulation, an EU regulation that mandates data protection and privacy for all individuals within the European Union.
Green ICT Objectives	EU goals to minimize the environmental impact of digital infrastructure by promoting energy efficiency, sustainable data management, and eco-friendly practices.
High-Performance Computing (HPC)	Computing resources that enable data-intensive tasks and complex calculations, often necessary for large-scale research.
Metadata Harvesting	The collection of metadata across different platforms to ensure data discoverability and FAIR compliance, enhancing research data management.
Middleware Solutions	Software that connects different applications, data, or services, enabling interoperability and seamless data exchanges between platforms.
Service Aggregation	The process of collecting and organizing research tools, data, and services into a unified platform for easier access and discovery.
Service Registries	Tools for cataloguing and discovering available services within an ecosystem, helping users identify and access the resources they need.
Technology Readiness Level (TRL)	A scale used to assess the maturity of a technology, ranging from TRL 1 (basic principles observed) to TRL 9 (fully operational). IT Services in RESILIENCE are expected to meet TRL 9 for robustness.
Virtual Machines (VMs)	Virtualized computing environments that allow users to create isolated systems for research without requiring physical hardware.

5.2 IT Services Available Through EOSC EU Node Platform

An overview of key services offered through the **EOSC EU Node Platform**, including:

- **File Sync and Share**
- **Interactive Notebooks**
- **Large File Transfer**
- **Virtual Machines**
- **Cloud Container Platform**
- **Bulk Data Transfer**

6 Document Information

6.1 Reference Documents

Reference documents are intended to provide background and supplementary information.

ID	Date	Title/Reference
R1	18/08/2022	GRANT AGREEMENT Project 101079792 — RESILIENCE PPP
R2	22/02/2023	ITSERR – Stakeholders Analysis

Funded by
the European Union