JERICO-DS DELIVERABLE

Joint European Research Infrastructure of Coastal Observatories - Design Study

DELIVERABLE #, WP# and full title	JERICO-DS D9/D.3.3 - WP3 - "Preliminary Operation Plan for e-JERICO Service Delivery"
5 Key words	e_JERICO, Service, Operation, Plan
Lead beneficiary	RBINS
Lead Author	Legrand Sébastien
Co-authors	
Contributors	Juan Gabriel Fernández (SOCIB), Miguel Charcos Llorens (SOCIB), Juan Miguel Villoria (SOCIB), Ludovic Lepers (RBINS)
Submission date (dd/mm/yyyy)	31/01/2024

Nature

X R = Report, □ P = Prototype, □ D= Demonstrator, □ O = Other

Dissemination level :

X PU □ PP □ RE □ CO

PU = Public, PP = Restricted to other programme participants (including the Commission Services), RE = Restricted to a group specified by the consortium (including the Commission Services), CO = Confidential, only for members of the consortium (including the Commission Services)

GRANT N°: 951799
PROJECT ACRONYME : JERICO-DS
PROJECT NAME : Joint European Research Infrastructure network of Coastal Observatories - Design Study
COORDINATOR : Laurent DELAUNEY - Ifremer, France - design.jerico@ifremer.fr

DOCUMENT TECHNICAL DESCRIPTION

Document ID	JERICO-DS-WP3-D9/D3.3-310124_V1.0

REVISION HISTORY

Revision	Date	Modification	Author
V1.0	30/01/2024	Initial version	Sébastien Legrand
V1.1	31/01/2024	Final Version	

APPROVALS

	Name	Organisation	Date	Visa
Coordinator	Delauney Laurent	Ifremer	31/01/2024	Approved
WP Leaders	Juan Gabriel Fernandez	SOCIB	31/01/2024	approved
WP Leaders	Sébastien Legrand	RBINS	30/01/2024	approved

Diffusion list

Consortium beneficiaries	Third parties	Associated Partners	other
X		X	

According to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the 78-17 modified law of 6 January 1978, you have a right of access, rectification, erasure of your personal data and a right of restriction to the data processing. You can exercise your rights before the Ifremer data protection officer by mail at the following address: IFREMER – Délégué à la protection des données- Centre Bretagne – ZI de la Pointe du Diable – 29280 Plouzané - FRANCE or by email: dpo@ifremer.fr + design.jerico@ifremer.fr
Ifremer shall not hold your personal data for longer than necessary with regard to the purpose of the data processing and shall destroy it thereafter.

Table of Content

EXECUTIVE SUMMARY

Considering the operation phase as from the JERICO-CORE service design is crucial due to several compelling reasons. This approach places users' expectations and satisfactions at the heart of the design. It allows designers to anticipate potential challenges and to streamline processes. It enhances efficiency, success and sustainability of the delivered service. It ensures a smooth transition and seamless integration of the systems from the development phase to the operation phase. Moreover, considering the operation phase from the design facilitates the robust implementation of the access and security policies (Deliverable D3.1). Finally, it allows understanding the operational requirements and anticipating the requested resources. In brief, taking the operation phase into account during the design is imperative for the JERICO-CORE long-term success. It allows for anticipatory problem-solving, optimization of resources, enhancement of security, and ultimately results in a more resilient, user-friendly, and cost-effective IT service.

This "Preliminary operational plan for e-JERICO/JERICO-CORE service delivery" is a comprehensive guide explaining how ITIL best practices do seamlessly integrate and coordinate these different challenges. It considers the establishment of a service desk, efficient IT operations management, effective application management, thorough technical management, and meticulous IT facilities management. Furthermore, the plan outlines processes such as service portfolio and service catalogue management, information security management, knowledge management, release and deployment management, monitoring and event management, incident and problem management, user request fulfilment, and access management.

1. Introduction

The coastal ocean environments are important for our society because many communities depend to a large degree on oceans, seas, and coastal biodiversity for their livelihoods. They provide an inestimable source of economic, social, and cultural wealth. However, they are largely influenced by climate change and other local stressors such as pollution and overfishing. Understanding the impact of these global and local pressures requires managing and assessing observational marine and coastal data, models, and other resources involved in the creation, analysis, and management of reliable data.

To address this challenge in European Seas at different spatial and temporal scales, the **J**oint **E**uropean **R**esearch **I**nfrastructure network for **C**oastal **O**bservatory (JERICO) was established as an integrated pan-European multidisciplinary and multi-platform Research Infrastructure (RI) dedicated to develop a holistic appraisal of coastal marine system changes.

JERICO-RI therefore aims to provide an integrated solution in Europe to face the challenges of the coastal marine systems due to natural and anthropogenic stressors by supporting, with high-quality integrated data of the coastal areas and related services, European initiatives such as the EU Marine Strategy Framework Directive, the EU Water Framework Directive, the Regional Seas Conventions such as OSPAR and HELCOM and consortiums such as ICES, among others.

To reach these goals, several coastal marine RIs in Europe started JERICO in 2011 as a joint effort to perform a systematic approach to monitor, observe, explore, and analyse coastal marine systems in order to reach reliable information of their structure and functioning in the context of global change. This cooperation has been and is being pursued within a cluster of projects now for more than 10 years:

- JERICO (2011-2015, FP7) focused on harmonising and integrating infrastructures and technologies such as moorings, drifters, ferrybox and gliders and paved the way for JERICO-NEXT.
- JERICO-NEXT (2015-2019, H2020) strengthened and enlarged the JERICO network and the interconnection between physics, biogeochemistry and biology.
- JERICO-S3 (2020-2024, H2020) builds on JERICO-NEXT to enhance the current value and relevance of the JERICO-RI, through the implementation of the science and innovation strategy previously defined.
- JERICO-DS (2020-2023, H2020) supports the Design Study towards a structured operational European RI supported by the EU Member States (and associated members) and the European Commission (EC), and as a high-value RI at EU level as part of the European Strategy Forum on Research Infrastructures (ESFRI) roadmap.

The JERICO consortium is now an advanced community and aims to build and implement a sustained and efficient JERICO-RI. In its mission to provide valuable insights and recommendations to guide the ESFRI preparation phase in the early stages of the project, JERICO-DS will leverage EU and nations legacies with coastal national RIs, propose innovative design solutions and business plan scenarios, selecting the ones that would optimally respond to national strategies and the pan-EU strategy of JERICO-RI.

For this purpose, the community identified the need to create a **JERICO e-infrastructure**, formerly known as **e-JERICO,** that would support JERICO-RI activities. Two phases laid the foundation and the concepts for the full-scale technical development towards the ESFRI roadmap: a pilot phase and a design phase. As explained briefly below, these two phases happen during the JERICO-S3 and JERICO-DS projects.

First, the e-JERICO pilot was developed in the context of the JERICO-S3 project. This pilot, commonly referred to as the JERICO **Coastal Ocean Resource Environment** Pilot (**JERICO-CORE Pilot**), was designed to respond to the necessity of creating a common digital framework that includes a Virtual Research Environment (VRE) and Thematic Services (TS).

Following this initial pilot phase, the design phase was the responsibility of WP3 of JERICO-DS that studied the key aspects for the design, implementation, and operation of e-JERICO in the long term, based on the lessons learned from JERICO-CORE pilot. The interaction of the JERICO-RI team with the stakeholders was also key for the implementation and development of the roadmap from different perspectives including the collection of further requirements at different levels, from European to national and regional levels. Key aspects complemented the analysis of these requirements were access, and security policies, metrics, data management, and operation plans. This document entitled "**Preliminary operational Plan for e-JERICO service delivery - Deliverable D3.3**" presents the result of task 3.4 of JERICO-DS which was described as follows in the DoW:

> **Task 3.4: Preparation for e-JERICO operation (M12 - M36) (RBINS, SOCIB, Ifremer-CNRS, cnr-OGS, All nations)**
> This task will create the structure plan for e-JERICO operational capability. Agreements will be established with those JERICO-RI components, ranging from individual Institutions to Nations and Regions (Pilot Super Sites and Integrated Regional Sites as defined in JERICO-S3) that have capability for long-term sustainability, and can reliably contribute to service and data provision. Such agreements will be included in the final draft of the e-JERICO operational plan for delivery of services that will document the day-to-day management for effectively running e-JERICO. This day-to-day management will include specific details of (1) all the tasks required to maintain the e-infrastructure, (2) the partners responsible for each task, (3) the timeline for task completion and (4) financial resources available to maintain e-JERICO.

The development of this preliminary operational plan for e-JERICO has been matured along with the developments of the security and access policies (Task 3.2 - D3.1) the technical design of e-JERICO (task 3.3 - D3.2) and the design of the implementation roadmap (Task

3.7 - D3.5). These three deliverables form together the design of the JERICO-CORE service life cycle, and have influenced each other.

Considering the operation phase as from the JERICO-CORE service design is crucial due to several compelling reasons. This approach places users' expectations and satisfactions at the heart of the design. It allows designers to anticipate potential challenges and to streamline processes. It enhances efficiency, success and sustainability of the delivered service. It ensures a smooth transition and seamless integration of the systems from the development phase to the operation phase. Moreover, considering the operation phase from the design facilitates the robust implementation of the access and security policies (Deliverable D3.1). Finally, it allows understanding the operational requirements and anticipating the requested resources. In conclusion, taking the operation phase into account during the design is imperative for the JERICO-CORE long-term success. It allows for anticipatory problem-solving, optimization of resources, enhancement of security, and ultimately results in a more resilient, user-friendly, and cost-effective IT service.

The report is organised as follows:

- In section 2, the JERICO-CORE concept is presented as well as the main elements of the technological design and some elements of the implementation roadmap. It introduces the 5 stages of the JERICO-CORE lifecycle and defines 3 levels of ambition for JERICO-CORE (worst case, realistic case and optimal case). Finally, it presents the place of JERICO-CORE in the overall JERICO-RI organisation.
- Section 3 is the actual preliminary operation plan. It follows the ITIL V3 best practices. Of course, in this JERICO-DS project, it is prematurated to name partners in charge of the different tasks for operation or even signed concrete agreements with individual Institutes, nations and regions (as made for JERICO-CORE pilot in JERICO-S3). However, templates for agreements have been made available in the report annexe 1.

2. JERICO-CORE : from a concept to a implementation roadmap

2.1 JERICO-CORE concept

The JERICO-RI consortium (2022) has defined as the unified central hub of JERICO-RI to discover, access, manage and interact with JERICO-RI resources including services, datasets, software's, best practises, manuals, publications, organisations, projects, observatories, equipment's, data servers, e-libraries, support, trainings, and similar assets.

JERICO-CORE aims at improving coastal data and information FAIRness[1] by facilitating the development of services to support specialised thematic research activities and building synergies for coastal ocean resources and services between JERICO-RI and other international research data infrastructures.

As a one-stop-shop service, JERICO-CORE will provide users an optimal way to gain an integrated form of access to:

- Transnational Access to the JERICO-RI physical infrastructures (platforms and sensors) offered by the national coastal observatories and JERICO-RI technical expertise centres.
- Resources required to both harmonise and implement JERICO-RI data lifecycle management methodologies: Best Practices, tools and services, and e-training modules.
- Quality controlled data that is routinely acquired by the different national coastal observatories, following the FAIR principles.
- Added-value products and services (indicators, nowcasts, analysis, etc.) generated by each individual JERICO-RI thematic expertise centre; and
- Dedicated cloud computing resources and virtual research environments (hardware, software, VREs) allowing researchers to perform advanced analysis on multi-disciplinary, multi-scale, multi-domain, and multi-sensor data sets.

Consequently, JERICO-CORE is the central element through which JERICO-RI users will access all JERICO-RI products and services.

Figure 1 illustrates the complexity of the JERICO-CORE concept.

[1] https://www.go-fair.org/fair-principles/

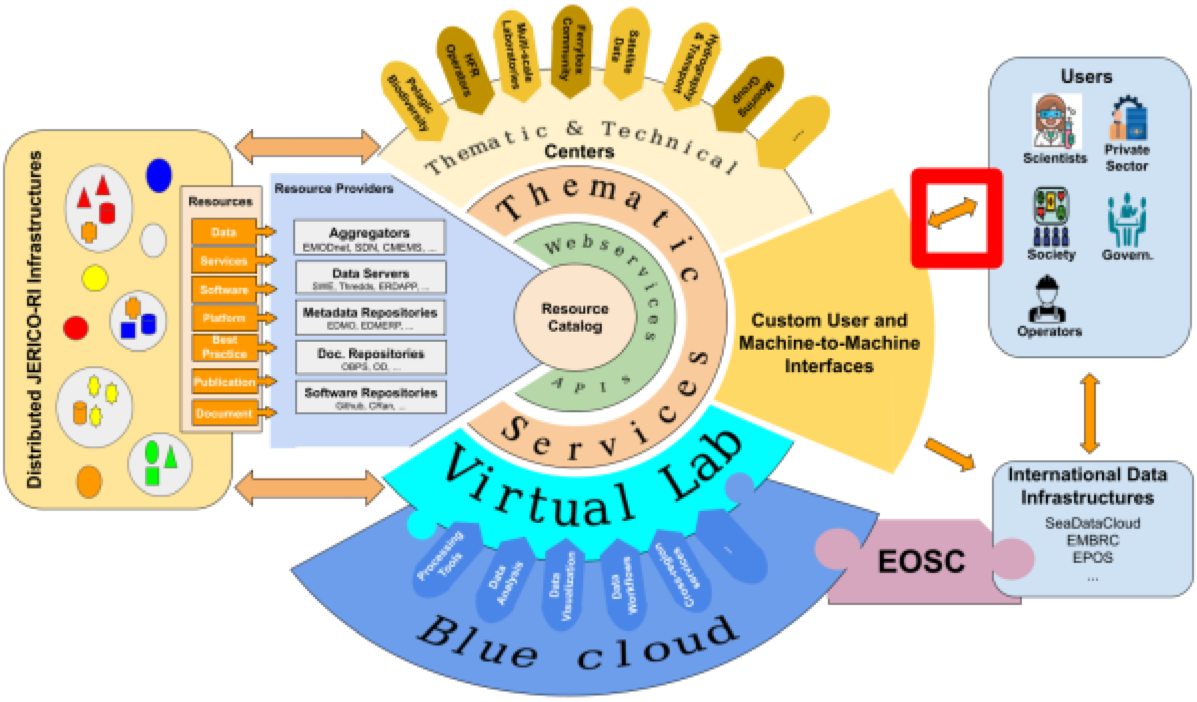

Figure 1 : Illustration of the complex JERICO-CORE concept.

Villoria et al. (2023) provides the following analyses on this concept:

"This concept deepens the connectivity between functional capabilities and services. Underlying the architecture is a flexibility to deal with innovation in science and engineering and meet new demands of users as new capabilities come online. It is designed to service current users and support evolution and growth for future needs. It must deal with the challenge that coastal resources are distributed among JERICO infrastructures using a diversity of standards and implementation methodologies. Resource providers collect these resources following workflows described and accepted in the ocean and coastal domain. However, there is not always a clear connection between the resources that are of a different nature. The JERICO-CORE infrastructure collects information about these resources through the existing providers of data, metadata, web services, software tools, documents and videos, among others. The information of these assets is interconnected in a knowledge base catalogue that is at the core of the infrastructure and offers a broad view on the data as well as observation and operation processes and capabilities in JERICO. The JERICO-CORE inventory represents the relation between the virtual and physical assets [...]. The cross-related nature of the information in the JERICO-CORE inventory facilitates the way resources are found and then accessed at the original source. Therefore, the knowledge of the relation between data, information, metadata, documentation, tools and workflows facilitates the traceability of assets and enhances the FAIRness of the data.

Furthermore, the concept includes a layer of thematic services that will support JERICO by helping the development of customised tools that use the available information. These tools are made available in a collaborative VRE supported by Blue-Cloud (https://www.blue-cloud.org). Tools are developed in this framework with direct access to the information and the access of JERICO-RI data, products and services. The access to the *resources of the catalogue will be provided via the JERICO-CORE REST API to support machine-to-machine interoperability. JERICO-CORE will support thematic and technical centres that are defined in the JERICO-RI structure. In the context of the EOSC, collaborative developments and improved access to resources, tools and services in a common infrastructure will enhance the collaboration with other research infrastructures. This two-way interoperability will benefit both JERICO and its stakeholders.``*

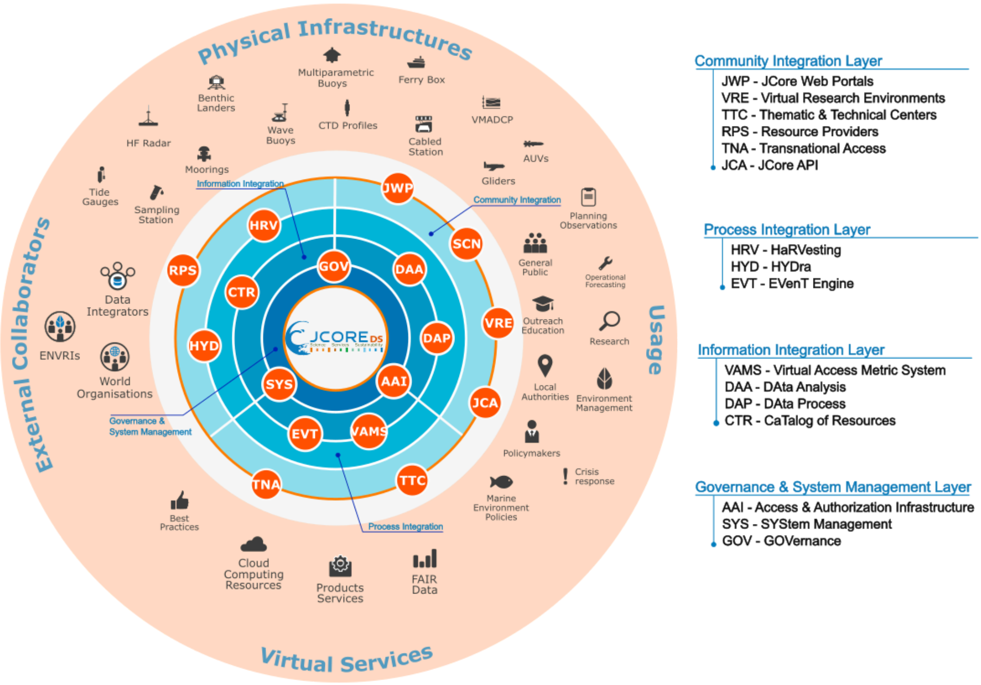

Figure 2 : Landscape view of the JERICO-CORE Service Architecture - JERICO-CORE is designed to interact around four main poles : Physical Infrastructures, Virtual Services, External Collaborators and Usage. For this, 16 service components, organised in 4 layers, have been identified (source: JERICO-DS Deliverable 3.2).

2.2 JERICO-CORE technological design

To produce the technological design, the JERICO-CORE concept has been reorganised to interact around 4 main poles : physical structures, virtual services, external collaborators, and usage (Figure 2). This reorganisation leads to the identification of 16 main service components organised in 4 service architecture layers (Figure 3):

- Community Integration Layer
  - JWP - JCORE Web Portal Services
  - VRE - Virtual Research Environment
  - TTC - Thematic and Technical Center Services
  - RPS - Resources Providers
  - TNA - Transnational Access to physical infrastructures
  - JCA - JCORE API
- Process Integration Layer
  - HRV - Data HaRvesting Service
  - HYD - HYDra (interaction with sensors at sea in real time)
  - EVT - EVenT Based Management service
- Information Integration Layer
  - VAMS - Virtual Access Metric System
  - DAA - DAta Analysis
  - DAP - DAta Processes
  - CTR - CaTalogue of Resources
- Governance and System Management Layer
  - AAI - Access & Authorization Infrastructure
  - SYS - System Management
  - GOV - Governance

The purpose of these 16 service components are explained in the JERICO-DS deliverable D3.2.

In a second step, various cloud platforms that could possibly host JERICO-CORE have been benchmarked against two sets of criteria. The first set evaluated technical and functional viability, ensuring the successful development of JERICO-CORE; the second set assessed development difficulty and associated technical and functional risks, highlighting uncertainties in project development. Deliverable D3.2 provides a detailed, scored analysis of these platforms, particularly focusing on their alignment with JERICO-CORE's main goal: integrating development with established research e-infrastructures.

The cloud services benchmark indicates that the Blue-Cloud infrastructure is currently the most suitable cloud platform to host the JERICO-CORE service.

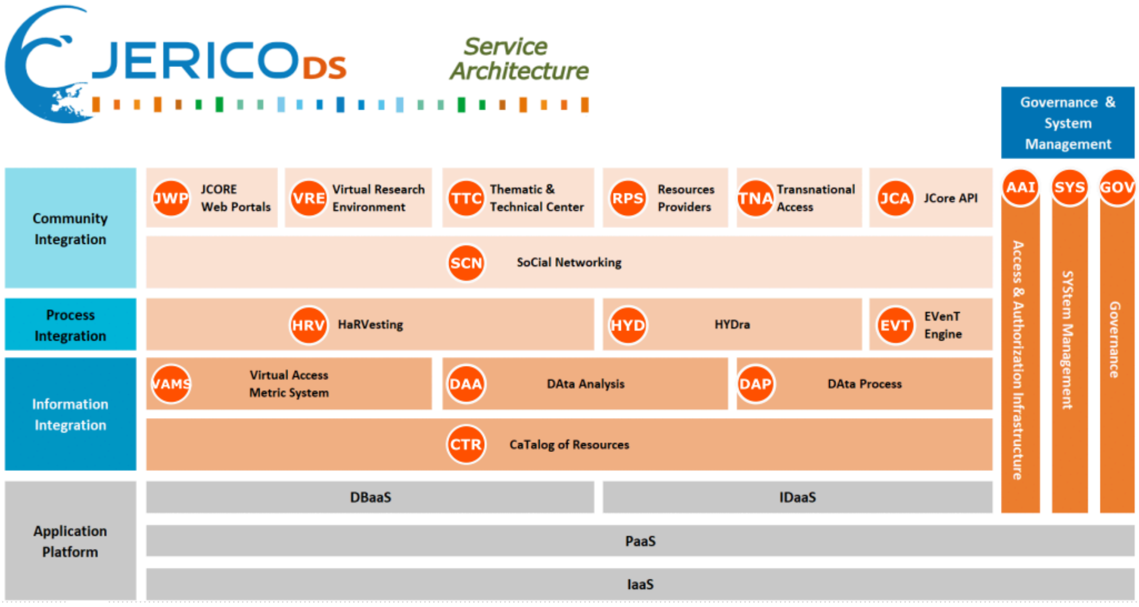

Figure 3 : Stacked view of the JERICO-CORE Service Architecture - 17 service components organised in 4 layers have been identified. The application platform layer is assumed to be operated by a third-party cloud service provider (source: JERICO-DS Deliverable 3.2).

2.3 JERICO-CORE life cycle and implementation roadmap

The JERICO-CORE implementation roadmap (JERICO-DS deliverable D3.5) details the key milestones that will have to be implemented throughout the 5 phases of the full JERICO-CORE life cycle, namely: the strategic design phase, the preparatory phase, the implementation phase, the operation phase and the closing phase (Figure 4).

The **strategic design phase** has been implemented jointly in the projects JERICO-S3 and JERICO-DS. Among others, this design phase includes understanding users and stakeholders expectations and requirements (JDS T3.1); defining the service policies (JDS-T3.2); shaping out the optimal technical design (JDS-T3.3); developing a strategic implementation roadmap (JDS-T3.7) and preparing from the very beginning the JERICO-CORE operation (JDS-T3.4).

The **preparatory phase** shall reply a series of concrete questions and issues that shall be solved before starting the JERICO-CORE implementation such as:

- How to add a service component in JERICO-CORE?
- How to decommission a service component?
- What are the service component metrics?
- What are the tools and technology required to implement the service component?
- Which architecture is required?
- What processes are required?
- What is the detailed budget?
- Which SLA are needed?
- How to document the service component?

- How to review the service component?
- How to monitor service component performance?
- How to maintain documentation and contracts?
- etc.

Three concrete milestones to be reached during this preparatory phase are the governance, teams and budget analysis; the requirement analysis and the final service design.

The **implementation phase** shall ensure that the actual development and deployment of the IT services will be carried out in a coordinated way. This covers every action to be done for the final design service before the operation. Typical questions to be handle in this phase are:

- Can the design be put in production directly?
- What if it is a large or complex implementation?
- Are any controls necessary before operations can begin?
- Which compliance checks?
- Which acceptance tests?
- How to ensure nothing breaks if some changes are required in operation later?
- How to ensure all the knowledge is transferred between developer teams and operation teams? More generally, how to ensure the knowledge is transferred throughout the full service lifecycle, including continuous improvement cycles and decommissioning?
- How to maintain information about hardware and software?
- etc

Key outcomes from this phase include the JERICO-CORE implementation document(s), the JERICO-CORE service manual(s), the implementation evaluation documents or the operational guides.

The **operational phase** of JERICO-CORE begins when the implemented infrastructure transitions into its fully functional state, making it accessible to the entire community. In contrast to the limited access during the implementation phase, the operational phase marks a significant milestone in the JERICO-RI ESFRI roadmap, as the infrastructure becomes widely available. The operational stage focuses on the daily work, i.e. fulfilling the users demands, monitoring service and handling the day to day issues and incidents. **Planning service operation is therefore answering questions such as:**

- How to organise the operations teams?
- What are their specific tasks? What must they deliver?
- Which skills, knowledge and resources do they need?
- etc

Detailing this JERICO-CORE operational plan is the purpose of the next section.

Finally the **closing phase** anticipates the decommission of some JERICO-CORE service components or even the JERICO-RI termination.

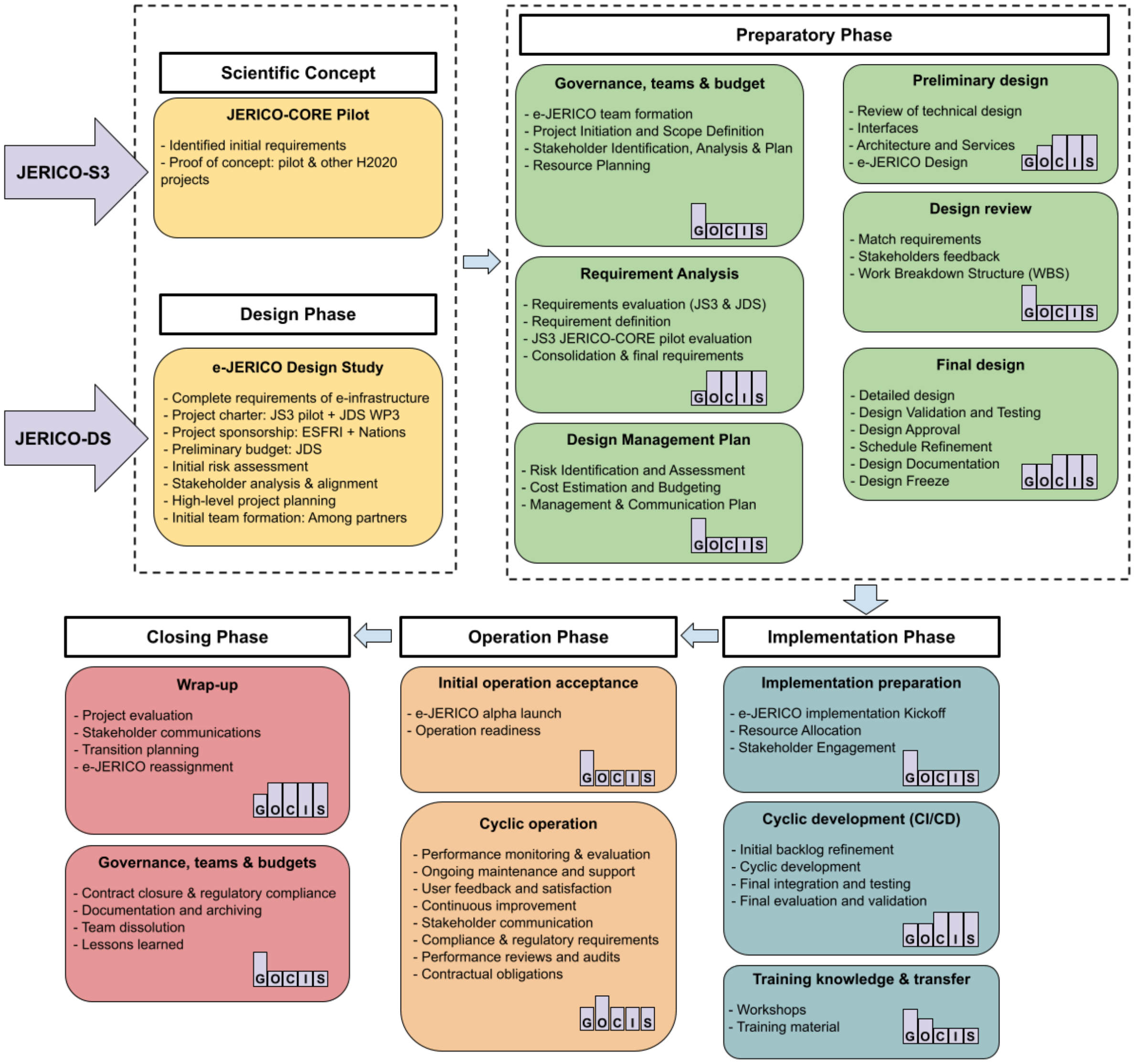
JERICO-S3
JERICO-DS
Scientific Concept
JERICO-CORE Pilot
- Identified initial requirements
- Proof of concept: pilot & other H2020 projects
Design Phase
e-JERICO Design Study
- Complete requirements of e-infrastructure
- Project charter: JS3 pilot + JDS WP3
- Project sponsorship: ESFRI + Nations
- Preliminary budget: JDS
- Initial risk assessment
- Stakeholder analysis & alignment
- High-level project planning
- Initial team formation: Among partners
Preparatory Phase
Governance, teams & budget
- e-JERICO team formation
- Project Initiation and Scope Definition
- Stakeholder Identification, Analysis & Plan
- Resource Planning
Requirement Analysis
- Requirements evaluation (JS3 & JDS)
- Requirement definition
- JS3 JERICO-CORE pilot evaluation
- Consolidation & final requirements
Design Management Plan
- Risk Identification and Assessment
- Cost Estimation and Budgeting
- Management & Communication Plan
Preliminary design
- Review of technical design
- Interfaces
- Architecture and Services
- e-JERICO Design
Design review
- Match requirements
- Stakeholders feedback
- Work Breakdown Structure (WBS)
Final design
- Detailed design
- Design Validation and Testing
- Design Approval
- Schedule Refinement
- Design Documentation
- Design Freeze
Implementation Phase
Implementation preparation
- e-JERICO implementation Kickoff
- Resource Allocation
- Stakeholder Engagement
Cyclic development (CI/CD)
- Initial backlog refinement
- Cyclic development
- Final integration and testing
- Final evaluation and validation
Training knowledge & transfer
- Workshops
- Training material
Operation Phase
Initial operation acceptance
- e-JERICO alpha launch
- Operation readiness
Cyclic operation
- Performance monitoring & evaluation
- Ongoing maintenance and support
- User feedback and satisfaction
- Continuous improvement
- Stakeholder communication
- Compliance & regulatory requirements
- Performance reviews and audits
- Contractual obligations
Closing Phase
Wrap-up
- Project evaluation
- Stakeholder communications
- Transition planning
- e-JERICO reassignment
Governance, teams & budgets
- Contract closure & regulatory compliance
- Documentation and archiving
- Team dissolution
- Lessons learned
G O C I S

Figure 4 : Overview of the JERICO-CORE implementation roadmap, spanning the 5 phases of the IT service life cycle (source: JERICO-DS Deliverable 3.5).

2.4 Budgeting JERICO-CORE : the three ambition levels approach

In a second step, the implementation roadmap (Deliverable D3.5) has been used to support the resource analysis and funding for JERICO-CORE development and operation. In view of JERICO-CORE complexity (Figure 3), three distinct scenarios for JERICO-CORE development have been envisaged, corresponding to three different level of ambitions for JERICO-CORE:

- the '**worst-case scenario**' assumes minimal funding, focusing on development based solely on the existing pilot project developed in the project JERICO-S3. This scenario represents the most constrained budget, where only basic functionalities are maintained. This scenario included the operation of 2 thematic services and harvest information from 2 data providers. The HYDRa component in the process integration layer is not developed.

- the '**medium/realistic case**' envisions a scenario where funding is adequate to meet the crucial requirements laid out by key stakeholders, balancing between cost and functionality. The budget assumed the integration and operation of 10 technical and thematic services, the harvesting of information from 10 large providers and the integration of 5 platforms in the HYDra layer (allowing real-time interactions between JERICO-RI and the integrated platforms). Data aggregators, JERICO-RI softwares and documents repositories as well as other international information systems are also integrated in JERICO-CORE.

- the '**maximum/optimal case scenario**' assumes the availability of ample funding, allowing for the comprehensive development of all planned requirements and functionalities: data and resources from all the JERICO-RI observatories are integrated in JERICO-CORE; up to 16 technical and thematic services are operated; 50+ platforms are interoperable in real time through the HYDra layer.

2.5 JERICO-CORE in JERICO-RI governance scheme

In the overall organisation of JERICO-RI as presented at the JERICO-DS final meeting in Novembre 2023, JERICO-CORE (e-JERICO) is located in the Expert Centre "Virtual Access" under the JERICO-RI Access Service Office.

The head of the Virtual Access Centre shall be a member of the JERICO-RI executive committee.

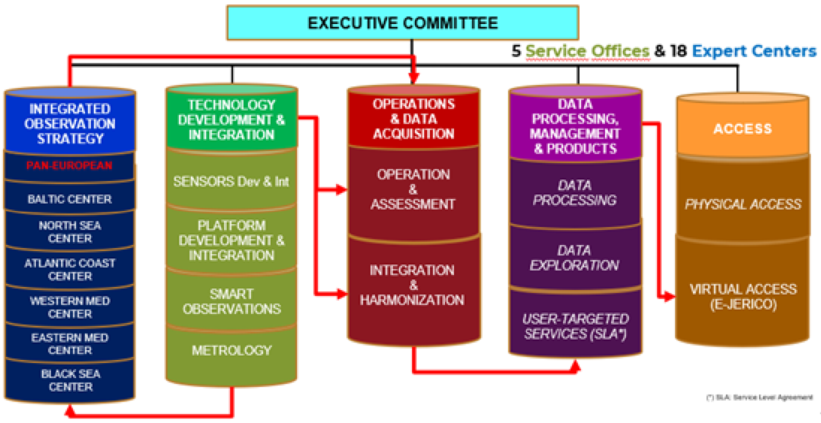
EXECUTIVE COMMITTEE
5 Service Offices & 18 Expert Centers
INTEGRATED OBSERVATION STRATEGY
PAN-EUROPEAN
BALTIC CENTER
NORTH SEA CENTER
ATLANTIC COAST CENTER
WESTERN MED CENTER
EASTERN MED CENTER
BLACK SEA CENTER
TECHNOLOGY DEVELOPMENT & INTEGRATION
SENSORS Dev & Int
PLATFORM DEVELOPMENT & INTEGRATION
SMART OBSERVATIONS
METROLOGY
OPERATIONS & DATA ACQUISITION
OPERATION & ASSESSMENT
INTEGRATION & HARMONIZATION
DATA PROCESSING, MANAGEMENT & PRODUCTS
DATA PROCESSING
DATA EXPLORATION
USER-TARGETED SERVICES (SLA*)
ACCESS
PHYSICAL ACCESS
VIRTUAL ACCESS (E-JERICO)
(*) SLA: Service Level Agreement

Figure 4 : The JERICO-RI governance scheme (as presented at the JERICO-DS final meeting in Novembre 2023) structures JERICO-RI activities into 5 different services offices and 18 expert centres. JERICO-CORE (aka E-JERICO) falls under the responsibility of the Access Office.

3. Preliminary Operation plan for JERICO-CORE

The objective of the JERICO-CORE preliminary operation plan is to identify all the elements that must be considered to prepare JERICO-CORE daily operations. Preparing service operation elements cover numerous dimensions as for instance interactions with users, suppliers and other 3rd party contractors; service level agreements and contract management; users and staff training; service monitoring; technical documentation; service maintenance; service assets management; service catalogue management; incident management; etc.

In addition, to ensure continuous improvement and user satisfaction, the operation plan must foresee robust feedback mechanisms, allowing JERICO-CORE users to provide valuable insights and suggestions. This feedback-driven approach enables ongoing refinement and optimization of JERICO-CORE to better meet the needs and expectations of its user community that will be collected by the JERICO User Committee. Along with security improvement, this user feedback mechanism should/shall drive JERICO-CORE continuous development cycles.

Several theoretical models and best practices exist to guide IT service management and operations. The dominant approaches are likely the ITIL best practices[2] and the ISO/IEC 20000 standard. In particular, ITIL V3 and ISO/IEC 20000 are interesting for our purpose as they follow the lifecycle approach used to define the JERICO-CORE implementation roadmap and defines 5 functions and 25 processes that should be put in place throughout the 5 lifecycle phases (cf. section 2.3).

This preliminary operational plan restricts itself to the functions and processes that have been identified as relevant in the JERICO-DS milestones document MS17 "Draft operational plan".

The identified ITIL functions are respectively

- JERICO-CORE service desk
- JERICO-CORE IT operation management
- JERICO-CORE application management
- JERICO-CORE technical management
- JERICO-CORE IT facilities management

The attributions of the first 2 functions deal with the day-to-day operation of the JERICO-CORE services, while the attributions of the last 3 functions cover several phases of the JERICO-CORE life cycle. In the operation phase, they do provide crucial support to solve problems and incidents.

[2] ITIL stands for Information Technology Infrastructure Library. It is a set of practices and guidelines for IT service management (ITSM) that focuses on aligning IT services with the needs of the business. ITIL provides a framework of best practices for planning, implementing, managing, operating and continually improving IT services. 4 versions of ITIL exist. In this report we consider ITIL V3, based on IT service lifecycle. ITIL V4 is mainly equivalent to ITIL V3, but best practices are presented in a context suitable for AGILE-like development.

Together, these 5 functions will act in a coordinated way to ensure a smooth and efficient operation of JERICO-CORE. To this purpose, ITIL best practices advices to organise the following processes :

- JERICO-CORE service portfolio and catalogue management
- JERICO-CORE information security management
- JERICO-CORE knowledge management
- JERICO-CORE release and deployment management
- JERICO-CORE monitoring and event management
- JERICO-CORE incident and problem management
- JERICO-CORE user request fulfilment
- JERICO-CORE access management

The preliminary operation plan of JERICO-CORE will therefore be organised in two different sections.

In section 3.1, the attributions of the different functions are carefully defined with a focus on the operation phase. The different functions in JERICO-RI governance schemes and a coarse estimation of the workload (in terms of FTEs) will be provided per phase and per JERICO-CORE ambition levels (worse case scenario, medium case scenario, optimal case scenario).

In section 3.2, the different processes organising the different attributions will be introduced. At the end of this JERICO Design Study project, only generic considerations can be developed. The actual processes organisation shall be discussed and documented in the future JERICO Preparation and Implementation projects.

3.1 Attribution of the different JERICO-CORE functions

In ITIL jargon, functions are specialised units responsible for the execution of specific tasks and processes, each function contributing to the overall effectiveness of the IT service delivery. ITIL V3 advises to organise an IT service operation around 5 main functions : service desk, technical management, application management, IT operation management and IT facilities management.

In this section, we explain the meaning of these 5 functions for the particular example of JERICO-CORE and suggest how these functions could be organised in the framework of 3 ambitions level JERICO-CORE (worst-case, medium case, maximum case) as defined in section 2.4.

3.1.1 JERICO-CORE service desk

The service desk is the primary point of contact between JERICO-CORE service providers and JERICO-CORE end-users. As it handles a wide range of inquiries (questions,assistance request, issues report, etc), the service desk must be perfectly aware of all the JERICO-CORE services but also the JERICO-RI experts that are behind these services. Because of this pivotal role, the service desk is in charge of a wide range of attributions.

User access management. The service desk manages the entire lifecycle of user access. Even if JERICO-CORE users will submit requests for access to JERICO-RI and manage their account via dedicated on-line tools, the service desk is in charge to review the access requests to ensure they are aligned with JERICO-CORE access and security policies; to grant access (i.e. configure users accounts, give right permissions levels, manage the list of accessible services, etc); maintain a detailed record of access requests and authorizations change, in accordance with JERICO-RI policies and regulatory requirements (GDPR, etc). For audit purposes, they also are in charge of periodic access review and monitoring. Finally they can also revocate users' access, a crucial role to prevent unauthorised and enforce security policy.

Communication and Information Distribution: The Service Desk serves as a communication hub, keeping users informed about the status of their reported inquiries. It also proactively distributes relevant information to users, such as planned service outages or changes in IT services. To this purpose, they will have to send individual emails, manage distribution mailing lists and maintain dedicated web pages.

Request Fulfilment: Beyond incident management, the Service Desk handles all type service requests. To this purpose, it may have to liaise e.g. with experts from JERICO-RI thematic and technical centres. It ensures that these requests are properly documented, processed, and fulfilled within agreed-upon service levels. A ticketing system is an important tool to efficiently track all the interactions with the users.

Incident and Problem Response : Service Desk escalates the reported incidents to IT Operation Management and keeps informed users of the progress until the resolution of the incident and the problem. Via this contribution, the service desk helps restore normal service operations as quickly as possible.

Knowledge Management: Service desk personnel contribute to building and maintaining a knowledge base that contains solutions to common issues, FAQs, and other relevant information such as manuals and training that documents any JERICO-CORE developments. It is also in charge that the information in the JERICO-CORE resources catalogue are complete and up-to-date. For this purpose, they will have to liaise with experts from all the JERICO-RI coastal observatories.

New service release. JERICO-CORE service desk staff must be perfectly trained and informed about the latest evolution of the JERICO-CORE service components. To this purpose, the service desk will review and validate the manuals and training that must be systemically delivered at the completion of all JERICO-CORE developments.

Organisation - Because of its pivotal role in JERICO-RI, the JERICO-CORE service desk must be part of the JERICO-RI Access Office.

Funding - Because of its pivotal role, the service desk should be funded by the nation's annual fees to JERICO-RI as well as by some overheads in the paid services delivered by JERICO-CORE.

Staff - The service desk must be adequately staffed to fulfil its missions. It will also have to scale with the number of JERICO-CORE users, the number of user inquiries handled by the service desk and finally the agreed service level agreement. As a coarse estimation:

- In the worst-case scenario, the service desk should be staffed by at least ½ FTE. With this level of resources, 80% of user inquiries should receive a first reply within the next 3 business days. The service desk is unattended during weekends, bank holidays, and for special events (sickness, meetings, training, etc). The service desk will also remain unattended for several consecutive weeks for staff holidays.
- In the medium case scenario, the service desk is staffed by at least 1.5 FTE. With this level of resources, any user request should receive a first reply within the next 2 business days. The service desk operates 52 weeks per year during business hours, but is unattended for weekends, bank-holidays and a few additional days per year (sickness, training, meetings, etc). The service desk is sufficiently staffed to handle planned holidays.
- In the optimal case scenario, the service desk is staffed by at least 3 FTE shared by at least 5 persons (1 FTE, and 4 ½ FTE). With this level of resources, any user request should receive a first reply by the next business day. The service desk operates 52 weeks a year during business hours. A person remains on duty during weekends and bank holidays to handle user reported incidents.

3.1.2 JERICO-CORE IT operations management

The IT operations management is in charge of executing the operational activities necessary to operate and manage JERICO-CORE on a day-to-day basis. Among others, it monitors and controls the IT services and IT infrastructure. IT Operations Management collaborates with the Service Desk, Application Management and Technical Management (including cloud service providers), to ensure seamless and continuous delivery of JERICO-CORE services. This coordination is essential for addressing incidents, implementing changes, and maintaining a well-functioning IT environment.

Operational Activities. IT Operations Management encompasses a wide range of operational activities to ensure the stability, reliability, and availability of JERICO-CORE services. This includes tasks such as job scheduling and batch processing, operation monitoring, backup and restore procedures, and routine maintenance activities:

- **Job Scheduling and batch processing.** This involves planning and scheduling various IT jobs, tasks, and processes to run at specific times or intervals. For instance, the job scheduling shall trigger the routine production of technical and thematic services. Efficient job scheduling helps optimise resource utilisation and ensures that critical tasks are performed in a timely manner. The Evt manager of the process integration layer (Figure 3) is the key tool to implement this attribution.
- **IT Infrastructure Monitoring.** IT Operations is responsible for monitoring the performance and health of the IT infrastructure. This includes servers, networks, storage, and other components. Monitoring tools are employed to detect and address issues proactively, minimising disruptions to services. A dedicated monitoring dashboard is a key tool to achieve this task. This dashboard must cover both cloud services (e.g. Blue-Cloud) and the key servers distributed among the JERICO-RI members.
- **IT Operations Control.** IT Operations Control involves managing and controlling the IT environment, ensuring that operational processes are executed according to established procedures. This function helps maintain the stability of IT services and responds to unexpected events or changes in the environment. A dashboard monitoring the key JERICO-CORE components (Figure 3) is key for this task. The dashboard shall monitor the Community Integration Layer (JWP, VRE, TTC, RPS, TNA, JCA), the Process Integration Layer (HRV, HYD, EVT), the Information Integration Layer (VAMS, DAA, DAP, CTR), Governance and System Management Layer (AAI, SYS, GOV)
- **Backup and Restore.** IT Operations is responsible for implementing and managing backup and restore procedures. This includes regular backups of critical data, systems, and configurations to ensure data integrity and the ability to recover from potential data loss or system failures. This is a crucial activity for the good implementation of the JERICO-CORE information security policy (cf. JERICO-DS deliverable D3.1); to avoid loss of information due to human errors, hardware failures or security attacks and to restore as fast as possible normal operation after a service outage.
- **Routine Maintenance.** IT Operations oversees routine maintenance tasks to keep IT systems and infrastructure in optimal condition. This may include applying patches and updates, performing system checks, and conducting preventive maintenance to prevent potential issues.

Incident and Problem Response. IT Operations Management shall coordinate all the response to detected or reported incidents and shall contribute to fix recurrent problems. For each open case, IT Operations Management is responsible for its logging, categorisation, documentation, handling, reviewing and closing. It quickly identifies the cause of incidents and problems. It implements temporary fixes or workarounds. It solves most 'simple' incidents and activates the IT technical and/or IT application managements for solving more 'complex' problems and incidents. It keeps the Service Desk informed of the incident resolution progress for good communication to users. In compliance with the security policy, all these tasks must be recorded within the Information Security Management System (ISMS) to support subsequent security risk analysis and improvements.

Knowledge Management: IT operations management contributes to building and maintaining a knowledge base that contains operation manuals, standard operating protocols, security risk assessments, contact lists, training, as well as any other relevant information useful to diagnose operations problems and fix them.

New service release. IT operations management must be perfectly trained and informed about the latest evolution of the JERICO-CORE service components. To this purpose, the service desk will review and validate SOPs, technical manuals, risk and security reports that must be systemically delivered at the completion of all JERICO-CORE developments.

Performance Monitoring and Optimization: Continuous monitoring of application performance is a key aspect. Application Management tracks metrics and KPIs, analyses trends, and identifies opportunities for optimization, ensuring that applications meet performance expectations and service level agreements. IT operations management also prepares reports for the JERICO-RI executive committee.

Organisation - The JERICO-CORE Operations Management must be part of the JERICO-RI Access Office.

Funding - As a central element of JERICO-CORE operation, the JERICO-CORE Operations Management shall be funded by the nation's annual fees to JERICO-RI as well as by some overheads in the paid services delivered by JERICO-CORE.

Staff - The JERICO-CORE Operations Management must be adequately staffed to fulfil its missions. At the difference of the service desk, the workload of JERICO-CORE Operations Management mainly depends on the complexity of the JERICO-CORE system and is less correlated to the growth of the users number :

- In the worst-case scenario, the JERICO-CORE system shall remain relatively simple. As a consequence, the expected workload of JERICO-CORE operations management should be limited. In this scenario, the operations management must not work on a 365/7 basis. However, unlike the service desk, operations management must work all year round and cannot afford interruptions because of long sickness leave or holidays. To handle this limitation, JERICO-CORE operation management should be at least staffed by 3 persons covering together a full-time equivalent in the worst-case scenario.
- In the medium case scenario, the complexity of the JERICO-CORE system increases as well as the number of routinely operated technical and thematic services. One may expect that the workload for operations management significantly increases. However, the operations management might still work only during business days with maybe a light on-call service organised for weekends and bank holidays. With these constraints in mind, JERICO-CORE operations management should be staffed by 2 or 3 FTEs, maybe splitted on 4 to 6 persons.
- In the optimal case scenario, JERICO-CORE delivers services to advanced operational users with expectations for 365/7 support. To enforce this service level, JERICO-CORE operations management should be staffed by at least a team of 5 FTEs. In that context, one may assume that the salaries for 2 FTEs are specifically paid by the extra fees supported by the advanced operational users.

3.1.3 JERICO-CORE application management

The JERICO-CORE application management (software) is responsible for managing the JERICO-CORE components in the applicative layers (Figure 3)

- "Governance and System Management",
- "Community integration",
- "Process Integration" and
- "Information Integration"

These applicative layers have been introduced in section 2.2 and are detailed in JERICO-DS deliverable D3.2. Application management plays a major role in designing, testing, and improvement of the JERICO-CORE applicative components. Application management is an ongoing activity as opposed to the application development which is typically a one-time set of activities to construct applications. The attributions of the JERICO-CORE application management in support of the JERICO-CORE operation covers the following processes:

Configuration Management: Application management manages the configuration and the updates of the applicative layers, maintaining accurate records of their components, versions, and dependencies. This is crucial for effective change management, troubleshooting, and ensuring consistency across the IT environment.

Deployment and Release Management: Application Management oversees the deployment and release of applications into the live environment. This involves planning, coordinating, and verifying that new or updated applications are introduced without disrupting existing services. Deployment and release can only occur after training of the service desk and IT operations management, including approval of the relevant documentation.

Incident and Problem Response: Application management is responsible for resolving incidents and problems related to applications that cannot be fixed by operations management. Application Management collaborates with the JERICO-CORE operation management to swiftly resolve the problems, minimise downtime, and restore normal service operations.

Security and Compliance: Ensuring the security of applications and compliance with relevant standards and regulations is a priority. Application Management implements security measures, conducts vulnerability assessments, and collaborates with other teams to address security concerns. This attribution also includes drafting security procedures for rapid incident resolution to minimise JERICO-CORE downtime during maintenance or due to security attacks, human errors and technical failures. Security audits might be a good practice to detect security vulnerabilities and possible improvements. This attribution contributes to the implementation of the JERICO-CORE security policy.

User Training and Support: Application Management provides user training and support to ensure that end-users can effectively utilise applications. This involves creating documentation, offering training sessions, and addressing user inquiries or issues forwarded by the service desk.

Change Management: The function is actively involved in change management processes related to applications. This includes assessing the impact of proposed changes, coordinating approvals, and ensuring that changes are implemented in a controlled and systematic manner.

Organisation - In medium and large IT organisations, application development and application management is usually addressed by distinct teams, as they involve different function profiles and technical skills. However, it is not a strict rule and for JERICO-CORE, it might be relevant to ask applications developers to be involved in the application management team.

Funding - JERICO-CORE application management is a key function to support JERICO-CORE operations, and should therefore be funded by the yearly nation fee to JERICO-RI.

Staff - As a conservative estimation, a total of 3 person months per year and per JERICO-CORE component is considered. As a consequence, the staff number will linearly increase with the total number of JERICO-CORE components and technical and thematic services operated.

3.1.4 JERICO-CORE technical management and IT facilities management

Next to application management, ITIL defines two hardware related functions that are crucial to enforce a stable, reliable and cost-effective service operation. These are the technical management and the IT facilities management.

The role of **technical management** is to provide the required in-depth resources and technical skills and expertises which are necessary to support the continuing operations of JERICO-CORE. Basically this function handles the JERICO-CORE hardware as well as the "application platform" layers (cf Figure 3) provided by the cloud platform as a service. The attributions of the JERICO-CORE technical management includes :

Technology planning, i.e. selection of the hardware and low-level software, their commissioning, and decommissioning.

Maintenance of the hardware, low-level software, networks, and other technical components so that JERICO-CORE can be robust, scalable and aligned with the JERICO-CORE requirements. Of course, the IT infrastructure design is made before the operation stage. Service desk, operation management and application management must be kept aware of any maintenance operation of the IT infrastructure that may have repercussions on the JERICO-CORE normal operation.

Capacity and performance management This attribution involves monitoring the systems performance, analysing trends and planning for capacity upgrades or adjustments. This attribution could alternatively be transferred to the JERICO-CORE operations management.

Security and availability management This attribution aims at developing and maintaining plans for a resilient JERICO-CORE, with eventually security and redundancy measures as well as procedures for rapid incident resolution to minimise JERICO-CORE downtime for maintenance or due to security attacks, human errors and technical failures. Security audits might be a good practice to detect security vulnerabilities and possible improvements. This attribution contributes to the implementation of the JERICO-CORE security policy.

Incident and problem resolution. The IT technical management must obviously be callable by and provide swift and efficient support to IT operations management whenever an incident and a problem is detected with the hardware, the low-level softwares, networks and other technical components.

The second hardware-related function is the **IT facilities management**. This function manages the physical environment where the IT infrastructure is located. This includes all aspects of managing the physical environment, as power supply, cooling, building access management and environmental monitoring.

These two hardware-related functions have been pooled together because JERICO-RI will not directly manage hardware related issues of JERICO-CORE. In the current technical design (JERICO-DS deliverable D3.2), the central components of JERICO-CORE are expected to be hosted by some cloud-based service such as Blue-Cloud while the decentralised components shall be hosted by the different Institutes and coastal observatories affiliated to JERICO-RI. As a consequence, the technical management and the IT facilities management functions shall be largely subcontracted and/or delegated to these actors. These functions must therefore be carefully and accurately described in the Operational Level Agreements (OLAs) and underpinning contracts (UCs). Annex 1 presents a summary of all the important sections and elements to be included in OLAs.

In view of the importance of these OLAs and UCs, they will be under the direct responsibility of the head of the JERICO-RI Access Office.

Organisation - Technical management and IT facilities management are organised through Operational Service Agreements and/or the underpinning contracts between JERICO-RI and the cloud service providers (e.g. Blue-Cloud). These agreements are the responsibility of the head of the JERICO-RI Access Office.

Funding - the JERICO-CORE OLAs and UCs should be funded by the nation's annual fees to JERICO-RI as well as by some overheads in the paid services delivered by JERICO-CORE.

Staff

- Worst-case scenario : staff is outsourced to some external cloud service provider (e.g. Blue-Cloud) or provided in-kind by the JERICO-RI member Institutes.
- Medium case scenario : staff is outsourced to some external cloud service provider (e.g. Blue-Cloud). A minimal budget is made available for supporting the hardware maintenance as well as for incident and problem management for the services distributed among the JERICO-RI members.
- Optimal case scenario : staff is outsourced to some external cloud service provider (e.g. Blue-Cloud). Hardware maintenance as well as incident and problem management for the services distributed among the JERICO-RI members are reimbursed based on real cost.

3.2 JERICO-CORE processes

In the previous section, we began by referring to ITIL best practices and ISO/IEC 20000 standards to identify the key functions necessary for operating the JERICO-CORE service, including their respective attributions and connections to the JERICO-CORE access and security policies. This overview does not yet offer an operational plan to ensure the smooth, efficient, and robust functioning of JERICO-CORE operations. To address this, it is crucial to systematically organise the various attributions of each function into sets of clearly defined and well-documented workflows and processes, each of them organising a series of core tasks following ITIL recommendations. For each task, it is essential to create a RACI matrix as well as a comprehensive list of tools and resources necessary for task completion.

The RACI matrix is a tool that helps define and communicate the role and responsibilities of team members that are involved in a task either as "Responsible" [R], "Accountable" [A], "Consulted" [C], or "Informed" [I].

The RACI matrix is typically presented as a table where tasks or processes are listed on one axis, and the roles are listed on the other axis. The intersections of the rows and columns indicate the specific responsibilities (R, A, C, I) for each role in relation to each task.

Achieving such a detailed operation plan should be the objective to reach at the end of the JERICO-RI implementation phase. In this preliminary operation plan, we will limit ourselves to describe the different processes and tasks from a generic point of view.

To enforce the JERICO-CORE operation, the following processes should at least be developed:

- JERICO-CORE service portfolio and catalogue management
- JERICO-CORE information security management
- JERICO-CORE knowledge management
- JERICO-CORE release and deployment management
- JERICO-CORE monitoring and event management
- JERICO-CORE incident and problem management
- JERICO-CORE user request fulfilment
- JERICO-CORE access management

3.2.1 JERICO-CORE service portfolio and service catalogue management

The **service portfolio management** aims

1. at defining new or changed services and determining the assets required to offer the service;
2. at submitting a change proposal to the change management (a process defined in the continual service improvement) and/or at initiating the design stage of the new service and
3. to periodically review the services offered.

The service portfolio manager handles a series of documentation including service charter, service models, change proposals, service portfolio review reports, etc. Service portfolio management manages the mid- and long-term evolution of the service catalogue delivered through JERICO-CORE. Outcome of the service portfolio is therefore an important driver for the service catalogue management, and the actual service operation.

Table 1 : Preliminary RACI matrix for the process "service portfolio management". This process drives JERICO-CORE service change, what ultimately drives JERICO-CORE operations changes.

Service Portfolio Mgmt	**Head access office**	**JERICO-RI Executive Committee**	**JERICO-CORE User committee**	**Application Mgmt**	**Technical Mgmt**
New service or service change definition	R,A	C	C	C	C
Change proposal	A	I	I	R	R
Services review	A	C	C	R	R

Service catalogue management ensures that a service catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally. Service Catalogue Management provides vital information for all other Service Management processes and is a key element in the implementation of the user access policy.

Related tasks to the service catalogue management includes:

- Service Definition: Define and document the details of each service delivered through JERICO-CORE, including its scope, features, functionalities, and any service level targets or commitments.
- Service Availability and Pricing: Specify the availability of each service and, if applicable, include pricing information. This helps users understand when a service is available and any associated costs.
- Service Categorisation: Categorize services based on their characteristics, purpose, and the needs of the users. This helps in organising the service catalogue and making it more user-friendly.
- Service Documentation: Create and maintain detailed documentation for each service, covering aspects such as service description, service level agreements (SLAs), operational procedures, and any dependencies on other services or components.
- Service Catalog Maintenance: Regularly review and update the service catalogue to reflect any changes in services, service levels, or other relevant information. This includes adding new services, retiring outdated ones, and modifying existing entries.
- User Communication: Communicate changes, additions, or retirements of services to relevant stakeholders, including end-users, IT staff, and management. Ensure that users are informed about available services and any updates to service offerings.

Table 2 : Preliminary RACI matrix for the process "service catalogue management".

Service catalogue Mgmt	JERICO-RI Executive Committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	End-users
Service definition	A	R	C	C		C
Service availability and pricing	A	R	C	C		
Service Categorisation		A, R	C	C		
Service Documentation		A	R	R		
Service Catalog Maintenance		A,R				
User Communication			A,R			C
Service Request Fulfilment	I		A,R	R		C
Service usage Monitoring	I	A			R	
Audit and Compliance	I	A				

- Service Request Fulfilment: Collaborate with Service Desk and other relevant teams to ensure that service requests can be fulfilled based on the information provided in the service catalogue. This involves aligning service descriptions with the actual fulfilment process.
- Service usage Monitoring: Monitor the performance and usage of services listed in the service catalogue. Gather data on service utilisation, user satisfaction, and adherence to SLAs.
- Audit and Compliance: Conduct periodic audits to ensure that the service catalogue is accurate, up-to-date, and in compliance with organisational policies and standards.

3.2.2 JERICO-CORE information security management

Information security management ensures the confidentiality, integrity and availability of an organisation's information, data and IT services. The JERICO-CORE security policy foresees the development of an information security management system that follows the principles of the ISO/IEC standards 27001-27005. The service operator must be adequately trained to apply an information security management system adapted for JERICO-CORE.

Related tasks to the information security management includes:

- Security Policy Development and Governance: Develop and maintain information security policies that outline the organisation's approach to safeguarding information assets. These policies provide a framework for secure practices and behaviours.
- Security Governance: Establish a governance framework for information security, ensuring that responsibilities are clearly defined, and oversight mechanisms are in place to monitor and manage the effectiveness of security controls.
- Risk Assessment: Conduct regular risk assessments to identify potential threats, vulnerabilities, and risks to information assets. Evaluate the impact and likelihood of these risks and prioritise them based on their significance to the organisation.
- Risk Mitigation and Treatment: Develop strategies and plans to mitigate identified risks. This may involve implementing security controls, adopting encryption measures, establishing access controls, or implementing other security measures to reduce the risk to an acceptable level.
- Security Incident Management: Establish procedures for detecting, reporting, and responding to security incidents. This includes defining incident response plans, conducting investigations, and taking corrective actions to prevent future incidents.
- Security Architecture and Design: Ensure that security is integrated into the design and architecture of IT systems, applications, and networks. This involves considering security requirements from the initial planning phases through implementation.
- Access Management: Define and manage access controls to ensure that only authorised individuals have access to sensitive information. This includes managing user accounts, permissions, and enforcing the principle of least privilege. This task is further developed as a process in section 3.2.8.
- Security Auditing and Compliance: Conduct regular security audits and assessments to ensure that the organisation's information security measures comply with industry regulations, legal requirements, and internal policies.

- Incident Response Planning: Develop and maintain incident response plans to guide the organisation in effectively responding to and recovering from security incidents. This includes defining roles, responsibilities, and communication strategies during incidents.

Table 3 : Preliminary RACI matrix for the process "information security management".

Information security Mgmt	JERICO-RI Executive Committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	Development Mgmt
Security Policy Development	A, R	R	C	C	C	C
Security Governance	A,R	R	C	C	C	C
Risk Assessment	I	A,R	R	R	R	R
Risk Mitigation and Treatment	I	A	R	R	R	R
Security Awareness Training	A	R	R	R	R	R
Security Incident Management	I	A	R	R	R	R

Security Architecture and Design	I	A	I,C	R	R	R
Access Management	I	A	R	I	I	I
Security Auditing and Compliance	A	R				
Incident Response Planning	I	A,R	R	R	R	C
Security Monitoring		A	R	R	R	R
Security Perf. Metrics and reporting	I	A,R	I,C	R	I,C	I,C

- Security Monitoring: Implement monitoring tools and processes to continuously monitor the JERICO-CORE environment for security incidents or anomalies. This includes real-time monitoring of logs, network traffic, and other relevant security indicators.
- Security Performance Metrics and Reporting: Define and track key performance indicators (KPIs) and metrics related to information security. Generate regular reports to communicate the status of information security measures to relevant stakeholders.

3.2.3 JERICO-CORE knowledge management

Knowledge management aims to gather, analyse, store and share knowledge and information across the different JERICO-CORE actors and stakeholders. The goal is to ensure that valuable information and expertise are available to support decision-making, problem-solving, and the improvement of IT services. It improves efficiency by reducing the need to rediscover knowledge. A knowledge management system might be a good technical solution to transfer knowledge between developers and service operators.

Related tasks to knowledge management includes:

- Knowledge Capture: Identify, capture, and document valuable knowledge and information from various sources, including individuals, documents, incident records, and problem resolutions.
- Knowledge Validation: Validate the accuracy and reliability of knowledge articles. Ensure that information is relevant, complete and up-to-date.
- Knowledge Storage and retrieval: Establish a centralised repository or knowledge base to store and organise knowledge documents, FAQs, and other relevant information. Implement a structured and searchable format for easy retrieval.
- Knowledge Integration with Other Processes: Integrate knowledge management with other ITIL processes, such as Incident Management, Problem Management, Change Management, and Service Desk. Ensure that knowledge is effectively used to improve these processes.

Table 4: Preliminary RACI matrix for the process "knowledge management".

Knowledge Mgmt	**Head access office**	**Service Desk**	**Application and technical Mgmt**	**Operations Mgmt**	**Development Mgmt**
Knowledge capture	A	R	R	R	R
Knowledge validation	A	R	R	R	C,I
Knowledge storage and retrieval	A	R		R	
Knowledge Integration within other processes	A	R	R	R	C,I

3.2.4 JERICO-CORE release and deployment management

The release and deployment management involves the coordination and execution of planned releases of software or hardware into the operational environment, ensuring smooth deployment and minimising disruptions. Release and deployment management organises the crucial movement of releases to test and live/operational environments. The primary goal of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release deployment is a crucial instant in the JERICO-CORE life cycle as it is the transition between the service developers and service operators. This presupposes that the release has been carefully planned and thoroughly tested and all the supporting and training documentation is available for the operators and users (knowledge management). It is advised to foresee an early life support period during which developers are available for fixing remaining errors and deficiencies as well as resolving any operational issues that have not been anticipated.

Release and deployment tasks that involved the operations teams include:

- Deployment Planning: Develop a deployment plan that outlines the steps and procedures for moving the release from the test environment to the live environment. This plan considers factors such as rollback procedures, communication plans, and contingency measures.

Table 5: Preliminary RACI matrix for the process "release and deployment management".

Release and deployment Mgmt	JERICO-RI executive committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	Development Mgmt	end-users
Deployment planning	I	C, I	C, I	C, I	C, I	A, R	I
Deployment execution		C, I	C, I	R	R	A, R	
Communication and Coordination		I	A,R	I	I	R	I
Backout planning		I	I	C,I	C,I	A,R	

Post-deployment review	I	R	R	R	R	A,R	
Documentation and knowledge		I	R	C, I	R	A, R	I

- Deployment Execution: Execute the deployment plan in a controlled manner. This involves installing, configuring, and activating the release components in the live environment while minimising the impact on ongoing business operations.
- Communication and Coordination: Communicate with stakeholders, including end-users, IT teams, and JERICO-RI contributing experts, to provide information about the upcoming release and any associated changes. Coordinate activities to ensure a smooth deployment process.
- Backout Planning: Develop a backout plan to address any issues that may arise during or after the deployment. The backout plan defines the steps to revert to the previous state if the deployment is unsuccessful or if unexpected issues occur.
- Post-Deployment Review: Conduct a post-deployment review to evaluate the success of the release. Gather feedback from users and stakeholders, analyse any incidents or issues that occurred, and identify opportunities for improvement in future releases.
- Documentation and Knowledge Transfer: Update documentation, such as user guides, operational manuals, and SOPs to reflect changes introduced by the release. Ensure that relevant knowledge is transferred to support teams and end-users to facilitate effective use of the new or updated components.

3.2.5 JERICO-CORE monitoring and event management

Monitoring and event management process ensures all operations run smoothly and that each event is handled in a timely manner with the appropriate response. It makes sure configuration items and services are constantly monitored and events are appropriately handled. Events might be routine production tasks of the technical and thematic centres but also alerts or notifications created by any IT systems (hardware and software). These events trigger a series of actions according to their severity (information, warning, exception). The list of possible events must be categorised, duly logged, documented, handled in a timely manner, reviewed and closed.

Logged events are useful to periodically perform event trends analysis and patterns and define new actions to improve service reliability and security.

The monitoring and event management typically assumed the development of an event monitoring system (software). The list of possible events tracked by this system must be agreed by all the service operation actors. Once the events list is available, the monitoring and event management process can be subdivided into 4 subprocesses:

a. the Maintenance of Event Monitoring Mechanisms and Rules
b. Event filtering and correlation
c. Event handling and response
d. Event review and closure

Tasks related to the monitoring and event management includes:

- Monitoring Objectives Definitions: Clearly define the objectives of monitoring, outlining what aspects of the IT infrastructure and services need to be monitored. This may include servers, networks, applications, and other critical components.
- Critical Events Identification: Identify and define the critical events that should be monitored. This involves determining which events are indicative of potential issues or disruptions to IT services.
- Event Logging and Collection: Establish processes for logging and collecting events from various sources within the IT environment. This includes configuring monitoring tools to capture event data and store it in a centralised repository.

Table 6: Preliminary RACI matrix for the process "monitoring and events management".

Monitoring and events Mgmt	JERICO-RI executive committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	Development Mgmt	end-users
Monitoring Objectives Definiton	I	C, I	C, I	C, I	A, R	C, I	
Critical Events Identification		C, I	C, I	C, I	A, R	C, I	
Events logging			I	I, R	A, R	R	
Incident detection		I	R	I	A, R		

Escalation procedure			R	R	A,R		
Root Cause Analysis	I	A	C	C	R	C	
Performance monitoring		I	I	I	A, R	I	
Reporting & analysis	I	A	C, I	C	R	C	(I)
Continuous improvement		A, R	C	C	C	C	

- Incident Detection: Use event data to detect incidents or abnormalities in the IT infrastructure. This involves correlating events to identify potential issues and initiate incident management processes as needed. A detected incident raises an alert on the operations management dashboard.
- Escalation Procedures: Establish escalation procedures for events that cannot be resolved at the level of the JERICO-CORE Operations Management. Define clear paths for escalating events to higher levels of support or management, ensuring timely resolution. These escalation procedures usually involved the incident and problem management processes.
- Root Cause Analysis: Use event data to perform root cause analysis for incidents. Determine the underlying causes of problems and identify corrective actions to prevent future occurrences.
- Performance Monitoring: Monitor the performance of IT services and infrastructure components over time. Track key performance indicators (KPIs) to assess the health and efficiency of the IT environment.
- Reporting and Analysis: Generate reports on event data, including trends, patterns, and performance metrics. Analyse these reports to gain insights into the overall health and performance of the IT environment.

- Continuous Improvement: Regularly review and improve the Monitoring and Event Management process. Identify opportunities to enhance monitoring capabilities, update thresholds, and optimise the detection and response to events.

3.2.6 JERICO-CORE incident and problem management

In ITIL jargon, an incident is an unplanned interruption or reduction in quality of IT services, while a problem is the underlying cause of one or more incidents. Solving an incident is handled to restore as fast as possible the normal operation level while fixing a problem usually requires in-depth work. Incident and problem management are two different processes but share the same objectives of enforcing the JERICO-CORE security policy. They must be an integral part of the JERICO-CORE Information Security Management System as presented in JERICO-DS deliverable D3.1.

The objective of the **Incident management** is to manage the lifecycle of all incidents in order to return to normal operation as fast as possible. Incidents are reported in numerous possible ways, including via the event monitoring system, a user report, a supplier report, etc. As for monitoring and event management, incident management must be rightly categorised, logged, documented, handled, reviewed and closed. In addition, users should be informed in a pro-active way of service failures as soon as they are known by the service desk, so that they can adjust themselves to interruptions. Tasks to manage an incident includes:

- Incident Identification: Detect and identify incidents promptly through various means, including user reports, automated monitoring tools, or alerts generated by other ITIL processes.

Table 7: Preliminary RACI matrix for the process "incident management".

Incident Mgmt	**JERICO-RI executive committee**	**Head access office**	**Service Desk**	**Application and technical Mgmt**	**Operations Mgmt**	**Development Mgmt**	**end-users**
Incident identification		(I)	C , I	C	A, R		
Incident logging			I	C	A, R		

Incident categorisation					A, R		
Incident priorisation				C	A, R		
Initial diagnosis and investigations				R	A, R		
Escalation procedures				C	A, R	C	
Incident resolution				R	A, R	(R)	
Workarounds				R	A, R	(R)	
Incident Closure		(I)	I	C	A, R	C	
Incident documentation			C	R	A, R	(R)	
User communication			A, R		C		I

Incident review and analysis		A, R	C	C	C	(C)	
Incidence Mgmt perf. reporting	I	A, R			R		
Integratio n in other ITIL processes		A			R		

- Incident Logging: Record all relevant details of the incident, including a description, affected services, date and time of occurrence, and any initial diagnostics performed. This information is typically captured in an incident record within the Incident Management system.
- Incident Categorisation: Categorise incidents based on their nature, characteristics, and impact. This categorisation helps in prioritising incidents and directing them to the appropriate support teams (i.e. application and/or technical management).
- Incident Prioritisation: Assign a priority level to each incident based on its impact on JERICO-CORE operations, urgency, and potential risks. Prioritisation ensures that critical incidents receive prompt attention.
- Initial Diagnosis and Investigation: Perform an initial diagnosis to determine the cause of the incident. This may involve analysing available information, reviewing logs, and utilising diagnostic tools to identify the root cause.
- Escalation Procedures: Determine and follow escalation procedures for incidents that require higher levels of expertise or management involvement. Ensure that incidents are escalated according to predefined criteria and timelines.
- Incident Resolution: Resolve the incident as quickly as possible, either through known solutions documented in the knowledge base or by engaging with appropriate support teams and resources. Communicate progress to the affected users during the resolution process.
- Workarounds: If an immediate resolution is not possible, implement temporary workarounds to restore services or minimise the impact on users while a permanent solution is being pursued.
- Closure and Resolution Confirmation: Close the incident record once the issue is fully resolved and services are restored to normal operation. Confirm resolution with the affected users and ensure that they are satisfied with the outcome.

- Incident Documentation: Document the details of the incident, including the actions taken, root cause analysis, and any lessons learned. This information contributes to the knowledge base and aids in future incident prevention.
- User Communication: Communicate with affected users throughout the incident lifecycle, providing updates on progress, expected resolution times, and any relevant information. Maintain transparency and manage user expectations.
- Incident Review and Analysis: Conduct post-incident reviews to analyse the effectiveness of the incident management process. Identify areas for improvement, update documentation, and implement changes to prevent similar incidents in the future.
- Performance Reporting: Generate reports on incident management performance, including metrics such as incident volume, resolution times, and user satisfaction. Use these reports for continuous improvement and reporting to management.
- Integration with Other ITIL Processes: Integrate incident management with other ITIL processes, such as Problem Management and Change Management, to ensure a coordinated approach to addressing incidents, identifying underlying problems, and implementing changes to prevent recurrence.

Problem management seeks to minimise the adverse impact of Incidents by preventing Incidents from happening, meaning establishing a stable IT infrastructure and improving service and application. For Incidents that have already occurred, Problem Management tries to prevent these Incidents from happening again. While incident management is coordinated by JERICO-CORE operations management, the problem management shall be coordinated by the head of the access office. Problem management includes:

- Problem Identification: Identify and log problems based on patterns observed in incidents, recurring issues, or through proactive analysis of the IT environment. Problems are identified by analysing incident data and looking for commonalities.
- Problem Logging: Record details of identified problems, including a description, affected services, date and time of identification, and any initial diagnostic information. This information is typically captured in a problem record within the Problem Management system.
- Problem Categorisation: Categorise problems based on their nature, characteristics, and impact. This categorisation helps in prioritising problems and directing them to the appropriate support or developer teams.
- Problem Prioritisation: Assign a priority level to each problem based on its impact on operations, urgency, and potential risks. Prioritisation ensures that critical problems receive prompt attention.

Table 8: Preliminary RACI matrix for the process "problem management".

Problem Mgmt	JERICO-RI executive committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	Development Mgmt	end-users

Problem identification		A, R	C , I	C	C	C	
Problem logging		A, R	I	R	I	R	
Problem categorisation		A, R					
Problem priorisation		A, R		C		C	
Root cause analysis		A		R		R	
Problem resolution (planning and implementation)		A	I	R	I	R	
Knowledge base update		A	C	R	C	R	
Problem Closure		A, R					

Problem documentation		A, R		R		R	
User communication		C	A, R	C		C	I
Problem review and analysis	I	A, R	C	C	C	C	
Integration in other ITIL processes		A, R					

- Root Cause Analysis: Conduct thorough root cause analysis to determine the underlying reasons for problems. This involves investigating the entire IT service lifecycle, identifying contributing factors, and understanding the relationships between incidents and problems.
- Problem Resolution Planning: Develop a problem resolution plan that outlines the steps and actions required to address the root cause of the problem. This plan may involve collaboration with other ITIL processes, such as Change Management.
- Change Implementation: Implement changes to address the root cause of the problem. Ensure that changes are tested, approved, and deployed in a controlled manner to prevent unintended consequences.
- Knowledge Base Update: Update the knowledge base with information about the identified problem, its root cause, and the resolution steps taken. This knowledge is valuable for future incident resolution and problem prevention.
- Closure and Confirmation: Close the problem record once the root cause has been addressed and verified. Confirm the resolution with the affected users and ensure that they are satisfied with the outcome.
- Problem Documentation: Document the details of the problem, including the actions taken, root cause analysis, and any lessons learned. This information contributes to the knowledge base and aids in future problem prevention.
- User Communication: Communicate with affected users and stakeholders throughout the problem lifecycle, providing updates on progress, expected resolution times, and any relevant information. Maintain transparency and manage expectations.

- Problem Review and Analysis: Conduct post-problem reviews to analyse the effectiveness of the problem management process. Identify areas for improvement, update documentation, and implement changes to prevent similar problems in the future.
- Integration with Other ITIL Processes: Integrate problem management with other ITIL processes, particularly Incident Management and Change Management, to ensure a coordinated approach to addressing incidents, identifying underlying problems, and implementing changes to prevent recurrence.

3.2.7 JERICO-CORE user request fulfilment

User request fulfilment covers a series of actions usually handled by the service desk. These actions could be resetting a password, giving information and advice, and as a follow in a series of actions to support users. As for events and incidents, all user requests should be categorised, logged, quickly and efficiently handled, reviewed and closed. Users request fulfilment help to avoid incidents and monitor user satisfaction. In some cases, users request fulfilment requires escalation or triggered some service improvements.

Table 9: Preliminary RACI matrix for the process "user request fulfilment".

User request Fulfilment	JERICO-RI executive committee	Head access office	Service Desk	Application and technical Mgmt	Operations Mgmt	Development Mgmt	end-users
User request logging			A, R				C
User Request catagorisation			A, R				
User request evaluation and fulfilment		(C)	A, R	(C)	(C)		I
User request closure		I	A, R	(I)	(I)		I

User requests review analysis and reporting	I	A, R	C				
Users satisfaction analysis	I	A	R				I
Integration with other ITIL process including service continuous improvement		A, R					

3.2.8 JERICO-CORE access management

Access management aims to grant authorised users the right to use a service, while preventing access to non-authorized users. This ITIL process implements the access and security policies. This process includes the maintenance of a catalogue of user roles and access profiles and the maintenance of the users database (including identity, contact details, roles, etc…). The latter database must be designed in accordance with GDPR and secure with high level security standards. Key tasks for access management includes:

- Development and maintenance of a users roles catalogue: The catalogue of users roles is an inventory of the JERICO-CORE service environment specifying for each entry the associated access rights, the level of permissions and responsibilities of the users. It is the reference document guiding the service desk for fulfilling user access requirements.
- Access Request Handling: Receive and process access requests from users. This may involve requests for new access, modifications to existing access, or removal of access rights. This may involve provisioning user accounts, assigning roles, and configuring permissions on systems, applications, or network resources.
- Access Review and Recertification: Conduct regular reviews of user access rights to ensure they are still necessary and appropriate. This helps in identifying and removing unnecessary or outdated access, reducing security risks.

- Password Management: Manage and enforce password policies, including password creation, expiration, and complexity requirements. Reset passwords for users who have forgotten them or in cases of potential security breaches. This task should be automated as much as possible.
- Access monitoring and reporting: Maintain logs of user access activities and regularly monitor access logs for suspicious or unauthorised behaviour. This helps in identifying and addressing potential security incidents.
- Incident Response for Access Issues: Respond promptly to incidents related to unauthorised access or other access-related issues. Investigate and take appropriate actions to mitigate security risks.

Table 10: Preliminary RACI matrix for the process "access management".

Access Mgmt	**JERICO-RI executive committee**	**Head access office**	**Service Desk**	**Application and technical Mgmt**	**Operations Mgmt**	**Development Mgmt**	**end-users**
Users role catalogue	A	R	C	C	C	C	
Access request handling		A	R				I
Access review and recertification		A, R	R				I
Password management							R
Access monitoring and reporting	I	A			R		

Incident response for access issue		A	I	R	R		I

3.3 Tools and resources

In sections 3.1 and 3.2, a comprehensive set of tools and management systems has been outlined as key resources for executing the functions and tasks proposed in this operation plan. These resources encompass a user database, a ticketing system, a backup system, an information security management system, a knowledge and information management system, a code versioning system, an automatic event logging system, an event and incident dashboard, and an incident management system or a problem management system.

The careful selection of appropriate tools and resources for different purposes will be a crucial consideration during the preparation phase. It's noteworthy that there are numerous standard solutions available at reasonable prices, and in some cases, even for free. For instance, widely-used ticketing systems like GLPI (by Teclib') and Atlassian JIRA offer robust functionalities. Similarly, OTRS solutions and Atlassian Confluence are common tools for implementing the various management systems mentioned earlier.

In the realm of code repository and versioning, GitHub and GitLab stand out as dominant global standard solutions. Additionally, libraries like log4j provide comprehensive functionalities for developing an automatic logging system tailored for JERICO-CORE. It's essential to explore these options during the preparation phase to align the selected tools with the specific needs and requirements of the operation plan.

4. Outreach, dissemination and communication activities

The purpose of this deliverable is to propose head principles according to which JERICO-CORE shall be operated. This preliminary operation plan shall be further refined in the JERICO-RI preparation and operation phases. For this reason, no specific outreach or communication action is necessary.

5. Conclusion and next steps

This "Preliminary operational plan for e-JERICO/JERICO-CORE service delivery" aims at being a comprehensive guide for the strategic implementation and operationalisation of the JERICO-CORE initiative.

First the document presented the key outcomes of the JERICO-CORE design, as matured during the JERICO-DS project. This provides an holistic overview that intricates access and security policies, technological design, implementation roadmap, budgeting considerations, as well as the integration within the governance scheme of JERICO-RI. All these elements shape the context and constraints in which JERICO-CORE shall be operated.

Integrating the ITIL best practices, the preliminary operation plan offers a meticulous breakdown of the attributions of different functions and processes vital to the success of JERICO-CORE. This includes, but is not limited to, the establishment of a service desk, efficient IT operations management, effective application management, thorough technical management, and meticulous IT facilities management. Furthermore, the plan outlines processes such as service portfolio and service catalogue management, information security management, knowledge management, release and deployment management, monitoring and event management, incident and problem management, user request fulfilment, and access management.

This detailed and organised approach ensures that each facet of JERICO-CORE is seamlessly aligned with the broader goals of JERICO-RI. By meticulously addressing the intricacies of each function and process, the plan sets the foundation for the effective coordination and functioning of JERICO-CORE. However, this Preliminary Operation Plan is only a starting point and numerous aspects shall be further developed during the JERICO-RI preparation and implementation phases.

6. References

- Legrand S. (2023) e-JERICO/JERICO-CORE Draft Operational Plan. Milestone report 17, JERICO-DS project, 18p.
- Legrand S., M. Charcos Llorens, J.M. Villoria, E. Breviere and J.G. Fernandez (2023) Outlined JERICO Virtual Resources Access and Security policies. Deliverable D3.1, JERICO-DS project, 26p.
- Villoria J.M., M. Ángel Alcalde, M. Charcos Llorens, J.G. Fernández, E. Reyes, J. Tintoré (2023) e-JERICO Technical Design Study. Deliverable D3.2, JERICO-DS project, 102p.
- Fernández J.G., C. Ramis Ferrer, J.M. Villoria, S. Legrand, P. Gorringe, E. Breviere, J. Mader, P. Gaughan, D. Durand, H. Wehde, L. Delauney, J. Tintoré (2024) Outlined e-JERICO Strategic Plan. Deliverable D3.5, JERICO-DS project, 56p.

- ITIL process wiki : https://wiki.en.it-processmaps.com/index.php/Main_Page, massively consulted between January 2023 and January 2024.
- Axelos Global Best Practice (2011) ITIL® Service Operation, second edition. TSO, London. ISBN 9780113313075.

Disclaimer

Insights and information were drawn from responses generated by the AI language model ChatGPT, developed by OpenAI. ChatGPT has primarily been utilised for enhancing and refining English through queries such as "please improve this piece of text: [...]" or "rewrite this piece of text in a more globish English". The resulting text has been adapted to suit the context of this report, with due credit given to the source.

Annexe

Annexe 1 : Template for Service Level Agreement (SLA) and Operational Level Agreement (OLA)

The website service level https://wiki.en.it-processmaps.com/index.php/Checklist_SLA_OLA proposes a generic template for service level agreement and operational level agreement.

These agreements should contain the following elements:

1. Service name
2. Clearance information (with location and date)
    a. Service Level Manager
    b. Customer representative
3. Contract duration
    a. Start and end dates
    b. Rules regarding renewal and termination of the agreement (if applicable, also rules regarding early termination of the agreement)
4. Description/ desired customer outcome
    a. Business justification and benefits
    b. Business processes/ activities on the customer side supported by the service
    c. Desired outcome in terms of utility (example: "Field staff can access enterprise applications xxx and yyy without being constrained by location or time")
    d. Desired outcome in terms of warranty (example: "High availability required during office hours in locations …")
5. Communication between customer and service provider
    a. Responsible contact person on customer side with contact details
    b. Designated Business Relationship Manager on service provider side with contact details
    c. Service Reporting (contents and intervals of service reports to be produced by the service provider)
    d. Procedure for handling exceptions and complaints (e.g. details to be included in formal complaints, agreed response times, escalation procedure)
    e. Satisfaction surveys (description of the procedure for measuring customer satisfaction on a regular basis)
    f. Service Reviews (description of the procedure for reviewing the service with the customer on a regular basis)
6. Service and asset criticality
    a. Identification of business-critical assets connected with the service
        i. Vital Business Functions (VBFs) supported by the service
        ii. Other critical assets used within the service (e.g. certain types of business data)
    b. Estimation of the business impact caused by a loss of the service or assets (in monetary terms, or using a classification scheme)
7. Service times
    a. Times when the service is required to be available
    b. Exceptions (e.g. weekends, public holidays)

8. Required types and levels of support
   a. On-site support
      i. Area/ locations
      ii. Types of users
      iii. Types of infrastructure to be supported
      iv. Reaction and resolution times (according to priorities, definition of priorities e.g. for the classification of Incidents)
   b. Remote support
      i. Area/ locations
      ii. Types of users (user groups granted access to the service)
      iii. Types of infrastructure to be supported
      iv. Reaction and resolution times (according to priorities, definition of priorities e.g. for the classification of Incidents)
9. Service level requirements/ targets
   a. Availability targets and commitments
      i. Conditions under which the service is considered to be unavailable (e.g. if the service is offered at several locations)
      ii. Availability targets (exact definition of how the agreed availability levels will be calculated, based on agreed service time and downtime)
      iii. Reliability targets (required by some customers, usually defined as MTBF (Mean Time Between Failures) or MTBSI (Mean Time Between Service Incidents))
      iv. Maintainability targets (required by some customers, usually defined as MTRS (Mean Time to Restore Service))
      v. Down times for maintenance (number of allowed down times, pre-notification periods)
      vi. Restrictions on maintenance, e.g. allowed maintenance windows, seasonal restrictions on maintenance, and procedures to announce planned service interruptions
      vii. Definitions of Major Incidents as well as Emergency Changes and Releases to resolve urgent issues, including procedures to announce unplanned service interruptions
      viii. Requirements regarding availability reporting
   b. Capacity/ performance targets and commitments
      i. Required capacity (lower/upper limit) for the service, e.g.
         1. Numbers and types of transactions
         2. Numbers and types of users
         3. Business cycles (daily, weekly) and seasonal variations
      ii. Response times from applications
      iii. Requirements for scalability (assumptions for the medium and long-term increase in workload and service utilisation)
      iv. Requirements regarding capacity and performance reporting
   c. Service Continuity commitments (availability of the service in the event of a disaster)
      i. Time within which a defined level of service must be re-established
      ii. Time within which normal service levels must be restored
10. Technical standards/ specification of the service interface

a. Mandated technical standards and specification of the technical service interface

11. Responsibilities
    a. Duties of the service provider
    b. Duties of the customer (contract partner for the service)
    c. Responsibilities of service users (e.g. with respect to IT security)
    d. IT Security aspects to be observed when using the service (if applicable, references to relevant IT Security Policies)
12. Pricing model
    a. Cost for the service provision
    b. Rules for penalties/ charge backs
13. Change history
14. List of annexes and references
15. Glossary