Deliverable D4.1

Helpdesk roadmap

Project Title Grant agreement no	**Genomic Data Infrastructure** Grant agreement 101081813
Project Acronym (EC Call)	GDI
WP No & Title	WP4: European Level Operations
WP Leaders	Christophe Trefois (5. UNILU)
Deliverable Lead Beneficiary	6. CSC
Contractual delivery date 30/04/2023	**Actual delivery date** 08/06/2023
Delayed	Yes
Partner(s) contributing to deliverable	(06. CSC)
Authors	Dylan Spalding (CSC)
Contributors	Francesca Morello (CSC), Laura KallioKoski (CSC)
Acknowledgements	NA
Reviewers	Rob Hooft (HRI), Mallory Freeberg (EMBL-EBI)

Log of changes

Date	Mvm	Who	Description
04/05/2023	0v1	Dylan Spalding (CSC)	Initial version
11/05/2023	0v2	Dylan Spalding (CSC)	WP4 reviewed version

08/06/2023	1v0	Dylan Spalding (CSC)	Final version following Management Board review

Table of contents

Contents

1. Executive Summary

This deliverable develops a roadmap for deploying both national and unified virtual helpdesks that coordinate internal (partners) and external (end-users) requests for support with the GDI infrastructure. It is proposed that the FitSM IT service management standard is used as a basis for the helpdesk as it supports federated scenarios, and a roadmap has been built to develop a helpdesk based on this, to be operational by April 2025. The roadmap will allow a constant flow of information between project partners via several communication tools and regulated by common SOPs, terms of use, and compliance with the GDPR requirements. In addition, knowledge exchange will be maintained with other operators of federated IT services to ensure best practice and aim for organisational interoperability with other projects and data spaces.
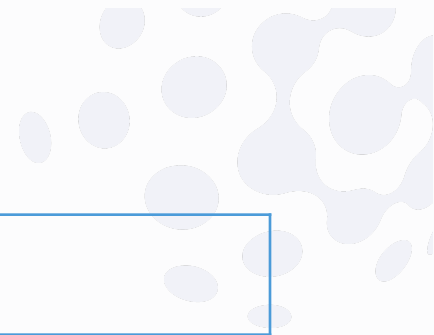
2. Contribution towards project outcomes

With this deliverable, the project has reached or the deliverable has contributed to the following project outcomes:

[Select 'Yes' (at least one) if the deliverable contributed to the key result, otherwise select 'No'. For more details of project outcomes, see here]

|	Contributed
Outcome 1 Secure federated infrastructure and data governance needed to enable sustainable and secure cross border linkage of genomic data sets in compliance with the relevant and agreed legal, ethical, quality and interoperability requirements and standards based on the progress achieved by the 1+MG initiative.	Yes
Outcome 2 Platform performing distributed analysis of genetic/genomic data and any linked clinical/phenotypic information; it should be based on the principle of federated access to data sources, include a federated/multi party authorisation and authentication system, and enable application of appropriate secure multi-party and/or high-end computing, AI and simulation techniques and resources.	No
Outcome 3 Clear description of the roles and responsibilities related to personal data and privacy protection, for humans and computers, applicable during project lifetime and after its finalisation.	No
Outcome 4 Business model including an uptake strategy explaining the motivation, patient incentives and conditions for all stakeholders at the different levels (national, European, global) to support the GDI towards its sustainability, including data controllers, patients, citizens, data users, service providers	Yes

(e.g., IT and biotech companies), healthcare systems and public authorities at large.	
Outcome 5 Sustained coordination mechanism for the GDI and for the GoE multi-country project launched in the context of the 1+MG initiative.	No
Outcome 6 Communication strategy – to be designed and implemented at the European and national levels.	Yes
Outcome 7 Capacity building measures necessary to ensure the establishment, sustainable operation, and successful uptake of the infrastructure.	Yes
Outcome 8 Financial support to the relevant stakeholders to enable extension, upgrade, creation and/or physical connection of further data sources beyond the project consortium or to implement the communication strategy and for capacity-building.	No

3. Methods

This deliverable describes the initial roadmap for the deployment of both national and centralised virtual helpdesks to support the stakeholders, customers, and use cases within the GDI. The intended structure of the helpdesk is given in Figure 1, whereby a centralised virtual helpdesk is formed from the helpdesks in each member state (node) . It is expected that there will be heterogeneity in operational requirements between the node helpdesks, so this deliverable concentrates on a roadmap to ensure that the European level, or virtual helpdesk, will become fully operational by 2025, providing a unified and consistent support service to customers and stakeholders, including technical, data management, and ethical guidance support. Such support is required to ensure the data within the European GDI are FAIR (Findable, Accessible, Interoperable, and Reusable), and that the infrastructure meets the requirements of both the 1+MG[1] Trust framework and applicable Ethical, Legal, and Societal Issues (ELSI) including the General Data Protection Regulation (GDPR)
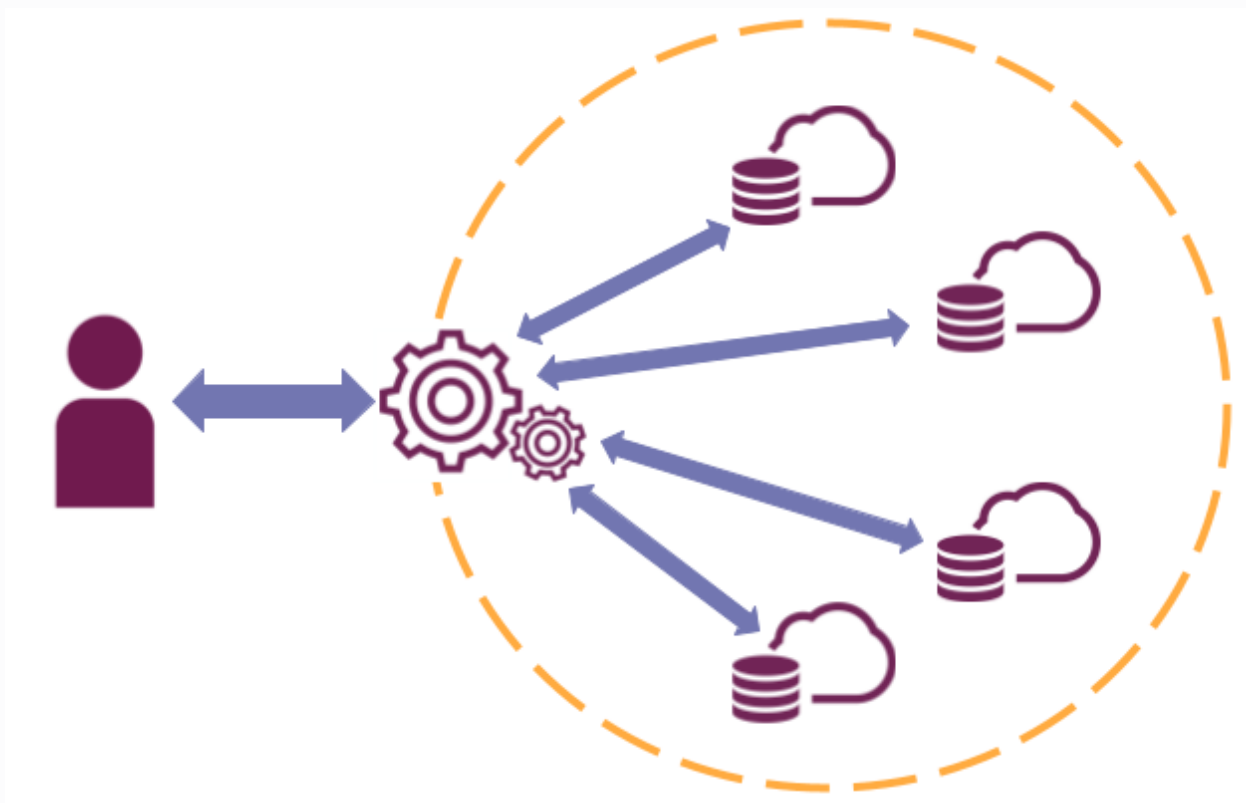
Figure 1. A single consistent, unified portal whereby a customer interacts with a virtual helpdesk, and requests are actually routed to and handled by composing national help desks.

Input was sought from other projects and infrastructures which run federated helpdesk, such as the Partnership for Advanced Computing[2] (PRACE), EuroHPC[3], and Federated European Genome-phenome Archive (FEGA), who operate federated helpdesks.

Having considered the relative scale of the federated helpdesk required for the European GDI when it is fully operational i9n 2026, investigation was made into standards that support the processes required for operation of a helpdesk, such as the ISO/IEC 20000-1[4] standard, which supporters federated scenarios.

3.1 Information Technology Service Management

Information Technology Service Management (ITSM) aims to provide high quality IT services which meet customers and users expectations by defining, establishing, and maintaining the process necessary to provide service management, for example the operation of a helpdesk. FitSM[5] is a collection of standards for lightweight ITSM, which is compatible with the ISO/IEC 20000-1[6] standard helping ensure IT Infrastructure Library[7] (ITIL) best practices are applied, which supports federated scenarios. It has four main principles - practicality, consistency, sufficiency, and extendibility. These principles support the ITSM foundations of service and customer orientation, process orientation, and continual improvement. The process model used by FitSM defines a set of processes that help enable the planning and delivery, or the operation and control, of IT services. In a federation, multiple parties or federation members, jointly contribute to the delivery of services to customers without being organised in a hierarchical setup or supply chain. Under this definition, GDI is a federation of nodes. Hence as distinct to a non-federated IT service provisioning model, the nodes collaboratively and jointly act as a service provider to form a supply network with the control over the service components and management processes distributed amongst the nodes, with the result that the SMS has less clear authorities and hierarchies than a non-federated IT service, resulting in more effort to clarify the responsibilities and interfaces between the nodes and service providers. This means that in a federated context, the documentation of processes and responsibilities are important, especially with respect to the operation of the virtual helpdesk.

---

[2] https://prace-ri.eu/
[3] https://eurohpc-ju.europa.eu/index_en
[4] https://www.iso.org/standard/70636.html
[5] https://www.fitsm.eu/
[6] https://www.iso.org/standard/70636.html
[7] https://wiki.en.it-processmaps.com/index.php/ITIL_4

Within FitSM, a *service* is defined as *a way to provide value to a user or customer by bringing about results that they want to achieve*. In the case of GDI, this could be discovery, access, and associated analysis of genomic data held within a node. As such the service provider (who delivers and manages) of that service must be defined. A process is the set of activities that achieve a specific result or objective, and these processes within ITSM are part of the service management system (SMS).

Within FitSM a procedure (or Standard Operating Procedure - SOP) is a set of steps or instructions that detail how to perform one or more activities within a process performed by an individual or team.

Within SMS there are four key roles as defined in Table 1.

Table 1. The four key roles defined in the FitSM standard.

Actor	Tasks / Responsibility
Service Owner	Primary contact for a service and has over responsibility for the service
Process Owner	Has accountability for the process
Process Manager	Responsible for the effectiveness of the process and is responsible to the process owner
Process Staff member	Responsible for performing the process and will escalate as required.

3.2 IT Service Management Processes

A process within FitSM consists of goals and objectives; the inputs, triggers, and outputs; the set of related activities that are provided by the services, and the roles and responsibilities of the actors. There are a set of 14 management processes within FitSM, outlined below. Each of the processes must be considered based on the type of IT service being managed, and the underlying infrastructure on which these services are deployed.

The **service portfolio** lists all the services provided by the service provider, for internal use within the GDI, and the service owner is responsible to ensure the list is current and kept up to date. Services

have a defined lifecycle, and this needs to be managed. This includes change management, for example new or changed services that are provided, major alterations to existing services.

The **service catalogue** is distinct from the service portfolio as it lists all customer facing live services, as well as relevant information on how to use them and what the required service level is for the service, or KPIs. For example, within the GDI nodes will each provide a set of services, and the performance of these services will affect the overall performance of the GDI. Hence minimum operational levels, or operational level agreements (OLAs), should be defined between service providers. These then can help identify where and when the GDI misses KPIs.

Both the above processes need to be supported by **service reporting** which can help decision making and support the demonstration of the required performance of the infrastructure. The frequency, audience, content, format and delivery of these reports need to be defined.

Defining the **service availability and continuity** is part of service availability and continuity management, and this includes risk assessment, generating service availability and continuity plans, as well as monitoring service availability. The requirements for SACM will come from the SLAs and OLAs where required.

Capacity management ensures that the infrastructure has the capacity to meet the customers requirements. This includes determining the requirements, how to monitor the utilisation of the infrastructure, planning for future capacity requirements (human, technical, and financial), and ensuring that capacity within the infrastructure does not become saturated.

Information security management ensures that the infrastructure corresponds to the ethical and legal requirements placed on the infrastructure, such as conformance to the General Data Protection Regulation (GDPR). This includes regular risk assessments, ensuring appropriate physical, technical, and organisational security controls are in place, and defining the policies and processes to ensure the confidentiality, integrity, and availability of the services and assets are maintained.

Customer relationship management aims to manage customer satisfaction (including complaint handling), ensure effective communication, provide a single point of contact with consistent user experience, and mechanisms for tracking and escalating customer issues.
Due to the set up of GDI the supplier relationship management is in general handled by the node internally, but should include processes to monitor supplier's performance, escalation methods, and maintenance of the communication channels.

Incident and service request management is the process of responding to user requests and restoring services, while incidents are defined as unplanned disruption of services. All incidents and

service requests must be registered, categorised, and prioritised, prior to resolution or fulfilled, based on any applicable SLA. Escalation of incidents or service requests, as well as their closure, should be consistent. Note that the SOPs required for incident management may overlap with those or other processes, such as information security management.

Problem management attempts to identify the problems, determine the root cause, identify any workaround, and if necessary initiate resolution via an RFC - part of change management. Problems must be registered and identified in a consistent manner, and actions identified to resolve or reduce their effect on the services.

Configuration management provides and maintains the logical model of items that contributes to the delivery of a service. This can include both technical components, such as hardware or software, and non-technical components, such as documentation or licences. A configuration item database is required to manage this - however this database need not be a single instance. This database will support the understanding and documenting of the configuration items, which themselves support the services.

Change management determines the processes for planning, approving,m and reviewing changes made to services to minimise disruption. The processes are initiated by a RFC that finally gets approved or not based on the appropriate SOP. RFCs, and associated changes, must be registered and classified, and dealt with in a consistent manner; including definition, impact assessment, level or approval required, post implementation review, and closure.
Release and deployment management are the processes used to change configuration items into a release, as well as the building, testing, evaluating, and accepting the releases. The methodology may include release cycles or continuous integration.

Continual service improvement aims to identify actions that will increase the performance or quality of a service. The inputs for this include the KPI and monitoring reports, service reviews, and feedback (both internal and external), and concerns both the services as well as the SMS that supports those services.

4. Description of work accomplished

4.1 Introduction

A summary of the data journey for data within the European GDI, that ensures the genomic and associated phenotypic and clinical data as FAIR (Findable, Accessible, Interoperable, Reuseable) as possible subject to the ELSI relating to these data, is given in Table 2, which is also mapped onto the five functionalities required for performing data analysis on genomic or phenotypic data - data discovery, data access management, data reception, storage and interfaces, and processing (Data Analysis). Each of these stages in the data journey must be supported by some form of technical support, or helpdesk. It is expected there will be two main actors interacting with the helpdesk, those within the GDI project and 1+MG use cases and stakeholders (Figure 2), and the external users, such as researchers who wish to utilise the data within the GDI.
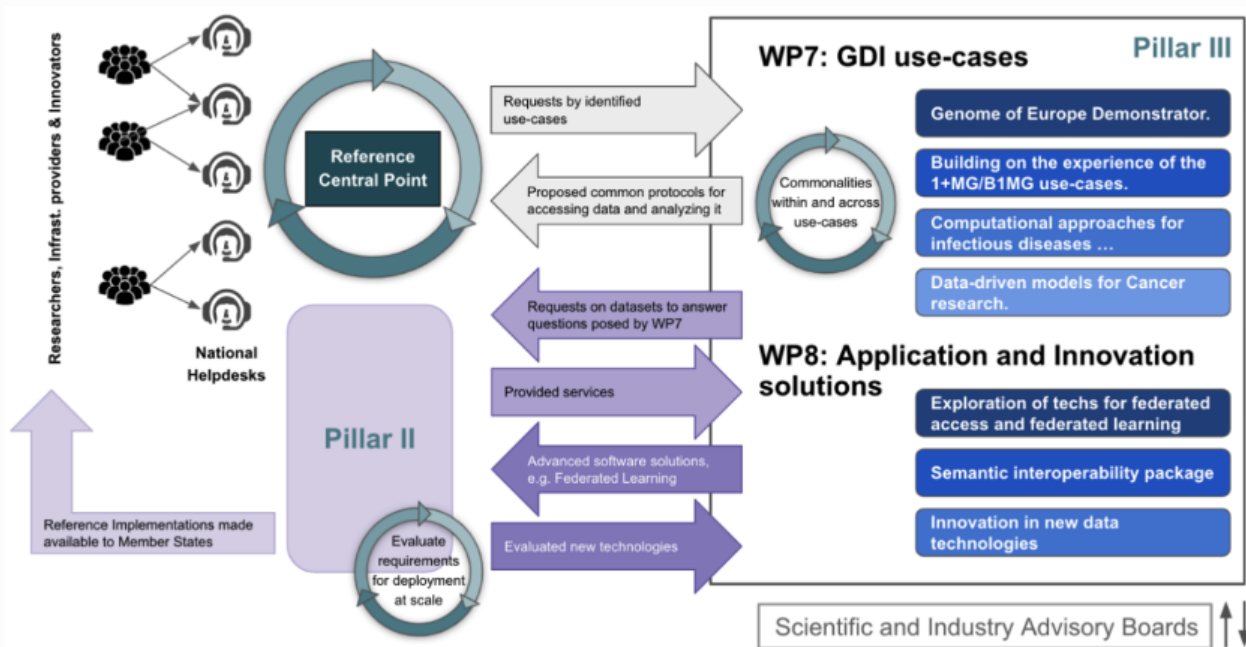

Figure 2: Diagram detailing the interactions between the use cases as well as scientific and industry advisory boards via Pillar III to Pillar II during the GDI project.

Table 2. Mapping the five functionalities supported by the European GDI onto the data journey. The helpdesk must support both the external users, who in general will discover, access, and use the data, as well as the GDI project and 1+MG users who will also prepare, include, and manage & store the data.

Data Journey		Data Infrastructure
Data	Pre-processing to agreed standards,	Data Reception

Preparation	annotation with metadata etc	
Data Inclusion	Physical transfer of data incl., legal transfer of data to 1+MG to enable visibility in data catalogue	
Data Storage & Management	Including GDPR Compliant processing environment, data versioning, backup etc	Storage and Interfaces
Data Discovery	Discovery of data using GDPR compliant APIs e.g., Beacon	Data Discovery
Data Access	A mechanism(s) by which the data controller can authorise access to select dataset(s)	Data Access Management Tools
Data Use	Data processing for the approved purposes	Data Processing

Each node or nodes, hosted in each participating country and containing data controlled by that country, must support the five functionalities required for performing data analysis on genomic or phenotypic data defined above. The proposed architecture enabling a node to provide these functionalities is given in Figure 2 below, including the supporting Global Alliance for Genomics and Health (GA4GH) standards, and an example research use case for access to the data.

4.2 National and virtual helpdesk

Users of the infrastructure being deployed by the GDI project should have a consistent user experience, and interact with a single point of contact. However in a federated infrastructure of national nodes each node should also set-up and operate their own helpdesk. Therefore it is proposed that a unified virtual helpdesk is set up formed from these national helpdesks. National helpdesks support end-users during the complete data journey (Table 1) data submission, discovery, permission management or service access. Moreover, provides feedback, maintains documentation, manages partners requests and coordinates with other nodes. A team of experts forms the helpdesk and operates using a ticketing system and other appropriate software to keep track of customer requests and distribute tasks between groups. Auditable records of end-users communications must be provided upon request and regulated by specific data retention policies.

The unified virtual helpdesk manages requests submitted via the GDI User Portal distributing them to the national helpdesks. The process of submission will need to be defined, but could be an email sent to the virtual helpdesk email list, or a page on the User Portal that contains a contact form. The virtual helpdesk requires implementation of a platform providing a single point of contact for users and allowing distribution/tracking of all requests/issues status. Access to the requests should be restricted, and processes and the tools required to ensure that tickets (a document for tracking and logging the process or workflow performed to satisfy the customer) are only accessible to interested parties must be developed. Additionally these tools and processes may need to support heterogeneity between nodes, as they interact with the national infrastructure, hence a survey of existing nodes regarding helpdesk operations and tools utilised is required to determine the level of heterogeneity. Any development of tools to support interoperability between these nodes must be part of WP3, where funds exist for software development and for the transition of nodes through from onboarding to operational.

An example list demonstrating the heterogeneity of tools and their purposes is:

- Request tracker system integrated with the User Portal or appropriate contact point,
- Project management platform (e.g. ZenHub) to distribute issues, track their status, collect feedback requests,
- Software management (e.g.GitHub),
- SOPs versioning and updates (e.g. ZenHub),
- Documentation versioning ad updates (e.g. GitHub),
- Communication with national nodes (mailing lists/ slack);

so depending on the outcome of the node helpdesk survey appropriate SOPs and, if necessary, interoperability tools will be created.

4.3 Helpdesk workflows and incident management

A proposed workflow for the virtual helpdesk is given in Figure 3. The external user will contact the virtual helpdesk, creating a helpdesk ticket but this process has to be defined in collaboration with the User Portal. However, the core underlying process should not rely totally on the User Portal for resilience, for example a form may be utilised on the User Portal but the underlying technology is an email that creates the ticket. This ticket will be classified, and subsequently assigned based on the classification. Depending on the assignee, the ticket may be passed to a node helpdesk or remain within the virtual helpdesk, however this process will be determined once the survey of nodes with existing helpdesk operations has been completed. The assigned helpdesk will follow the necessary

SOPs to satisfy the issue, and in the case of the node helpdesk the ticket will be passed back to the virtual helpdesk once the ticket is satisfied. An operator assigned to the virtual helpdesk will confirm within the external user if the ticket has been satisfied, and if so the ticket will be resolved, otherwise the ticket will be re-assigned depending on classification.
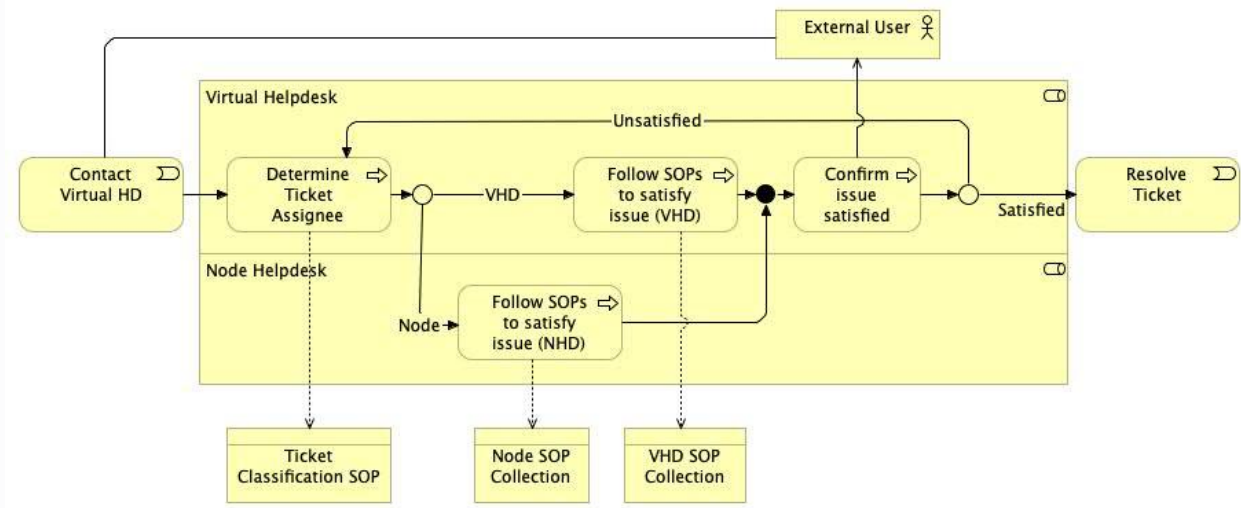

Figure 3. A proposed workflow for an external user interacting with the GDI virtual helpdesk. SOPs, ticket tracking and resolution, consistency of the user experience will all be defined based on the roadmap.

Daily work is carried out using a ticketing system to track according to standard operating procedures (SOPs) for:

- Ensuring tasks are consistently completed across nodes and transparent customer communication (user-facing SOPs).
- Efficient internal communication with support teams (operations, software development) for escalating tickets or tasks, incident management etc (node level SOPs) as well as node experts outside the support team such as legal support /contracts.
- Guaranteeing task implementation uniformity and reducing the risk of errors or omissions when coordinating work cia the virtual helpdesk (European level SOPs).

Helpdesk, whether virtual or node based, needs to support 3 levels of support, while level 0 support is provided by the user portal and level 4 by external actors, such as hardware vendors. The Level 1 HD provides the first line of support, logging issues, providing a single point of contact, describing processes and functions within the infrastructure. Level 2 helpdesk provides technical support and troubleshooting, as well as creating issues for identified bugs within the infrastructure. Level 3

provides expert support, such as architects and engineers who can also participate in the development of new software and processes.

4.4 Customer and user interactions

Figure 4 shows how Pillar III interacts with Pillar II. This methodology is required during the GDI project, to ensure that development requirements from the use cases and innovation solutions, routed via Pillar III, are combined with development requirements from users. Figure 5 shows how the interactions during the GDI project interact with Pillar III, which drives the development of solutions during the GDI project. The use cases interact, via Pillar III, with Level 3 HD who build the use cases and requirements for the infrastructure, and can also align these with the use cases and requirements from the external users which require new or updated features. Once the GDI project has deployed the European GDI, it would be expected that the use cases would interact with helpdesk in the more traditional manner, as external users and customers.

While the genomic and phenotypic data that will exist within the GDI project and subsequently the European GDI are one of the special categories of data under the GDPR, some of the metadata associated with these data, and associated to the operation of the European GDI, are also personal data and must conform to the GDPR (e.g. email addresses, IP addresses, names etc), for example by following the Data Protection by Design and Default[8] principles as the SOPs, processes, software, and tools are developed. Examples of issues that need to be considered are the generation of privacy notices for customers interacting with the helpdesk, tracking and logging of the personal data within tickets, and ensuring that these personal data are not stored longer than necessary, and SOPs on dealing with personal data entered into tickets, inadvertently or not. In a federated context consideration should be given to data minimisation, for example is it necessary that the contact details of the original requestor are passed to the different levels of support (e.g. from stage 2 to stage 3) as the request is acted upon, or can a method be found which maintains operational efficiency which minimising the transfer of personal data.

---

[8] https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en
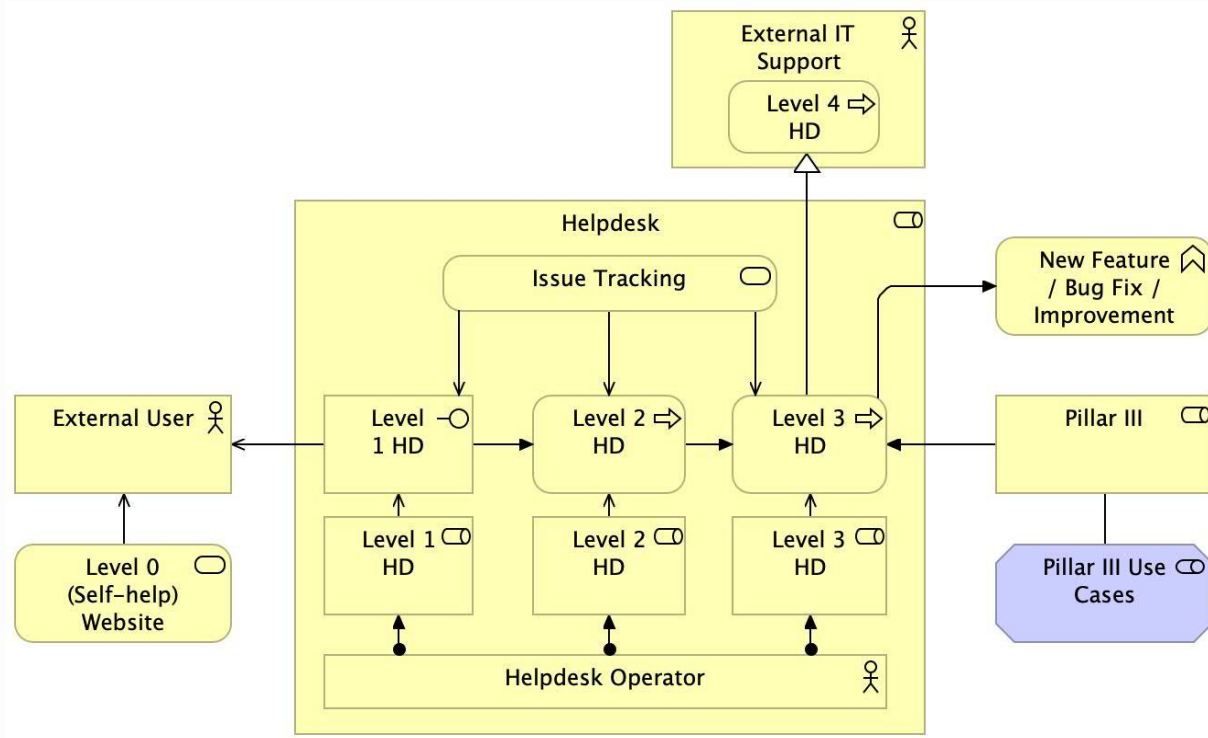
Figure 4. Helpdesk is composed of operators, who can act in one or more roles providing level 1 to level 3 support. An issue has to be tracked (as detailed in Figure 3) while the SOPs determine how, when, and why an issue should be escalated to different helpdesk levels.

5. Results

5.1 Roadmap Tasks

A set of roadmap tasks (added to the Gantt in Figure xx in Results) have been defined below (Table 3) which map onto the ITSM processes. Not all processes are based on the operation or control of the GDI, many are also involved in the planning and delivery of the infrastructure, and hence tend to be prerequisites for the operation and control processes. Additionally some processes may not need to be defined specifically within the GDI as they may be part of the node providing the services to the GDI - for example supplier relationship management may be part of the node responsibilities. However, monitoring, reporting, problem identification and escalation will still need to be identified within the GDI.

Table 3. Tasks for each specific management process within the federated infrastructure. The Who column determines who is responsible for the task, with 'N' indicating a Node level task, 'E' a European operations level task, and 'B' a task for the node and the European level operations.

Process	Process Code	Roadmap Tasks	Who
Service Portfolio Management	SPM	Survey existing node helpdesks Create service portfolio and lifecycle phases	E B
Service Level Management	SLM	Define service catalogue Generate knowledge base Define Service Level Agreements (SLAs), if necessary Define Operational Level Agreements (OLAs), if necessary Define service targets	B E E B B
Service Reporting	SRM	Define reports required	B
Service Availability and Continuity Management	SACM	Produce service availability and continuity plans to support SLAs / OLAs as required (with WP6) Monitor availability	B B
Capacity Management	CAPM	Define capacity plan Monitor utilisation of resources	N B
Information Security Management	ISM	Define specific security policies where required Create security risk assessment Document information security controls Generate privacy notices for each service utilising personal data	B B B B
Customer Relationship Management	CRM	Identify key customers and communication channels Define service review and complaint handling procedures	E E
Supplier Relationship Management	SUPPM	Define communication and monitoring procedures for suppliers	N
Incident Service Request Management	ISRM	Analyse current node level incident response procedures Create incident response protocols and procedures, including ticket tools and management based on DPbDD principles Create service request procedures	B B B

Problem Management	PM	Define procedures for problem management and identifying resources for resolution	B
Configuration Management	CONFM	Identify tools for configuration management Define procedures for configuration management, including controlling and tracking configuration items	N N
Change Management	CHM	Create procedures and workflows to deal with Request For Change (RFCs) Define change management authorities	B E
Release and Deployment Management	RDM	Define a release and deployment strategy Create monitoring and retrospective procedures for release and deployment actions	E E
Continual Service Improvement	CSI	Identify opportunities for improvement of services and SMS Ensure consistent evaluation of services and SMS Support onboarding of new nodes to operational status Survey other federated helpdesk operators	E E E E

Another operation of the helpdesk within the GDI project is to help support new nodes as they move from on-boarding, through deployment, to operational, which has been classified as part of continual service improvement as the nodes will transition at different rates, as detailed in the technical readiness level monitoring performed during the GDI project.. The SOPs developed in conjunction with the vanguard nodes (first set of nodes aiming to be operational in 2024) and the use cases in Pillar III, along with other stakeholders, will be utilised to create the outreach material and best practices for node operations. Virtual seminars will be held to help nodes as they become operational and link the national helpdesk to the virtual helpdesk as part of supporting the onboarding of new nodes.

Main tasks are in a Gantt chart[9]and with screen shots in Figures 5 to 8 below. These tasks are based on the FitSM standards for IT service management.
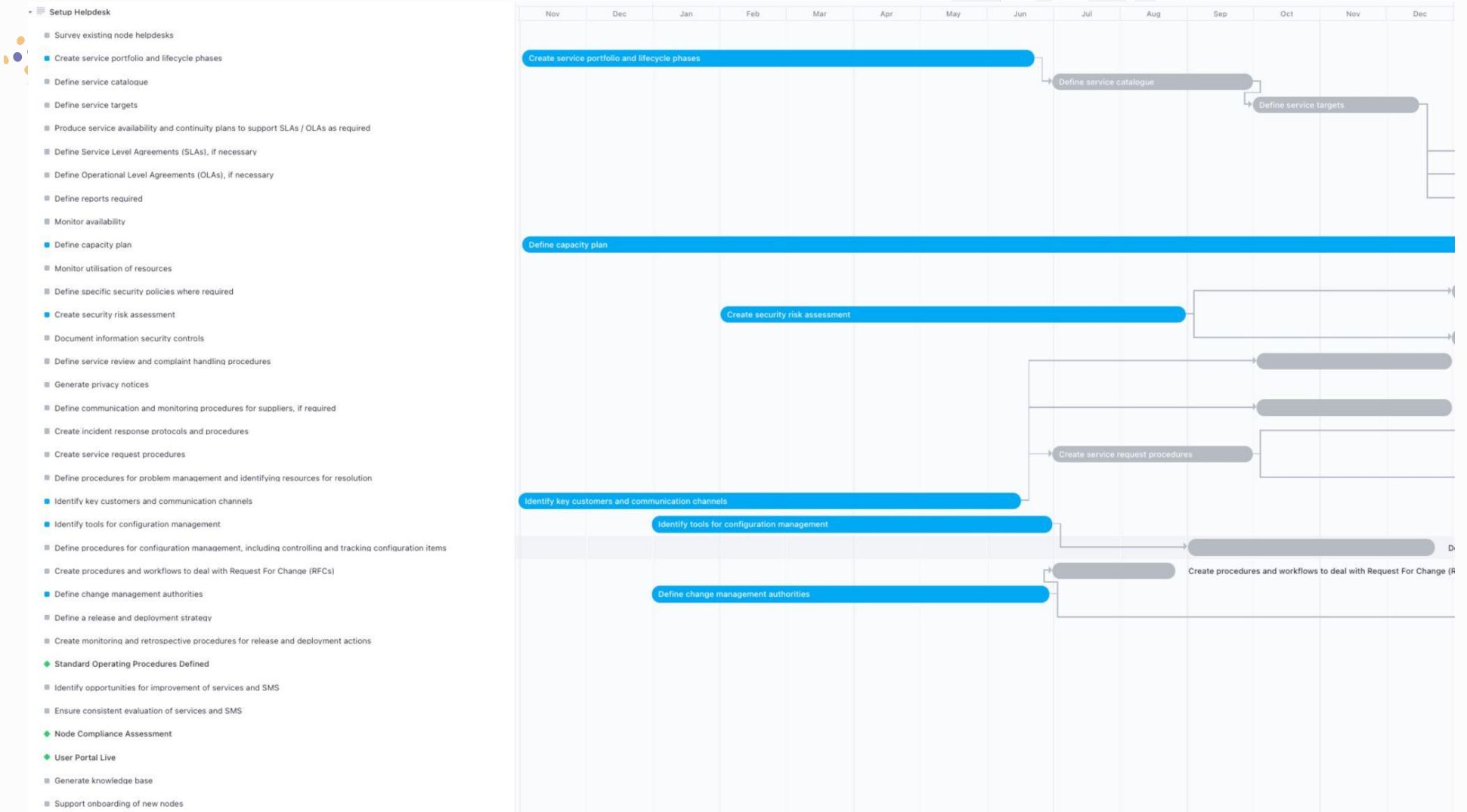
---

[9] https://sharing.clickup.com/9004101350/g/h/8cazbq6-61/14bdecd353961bf

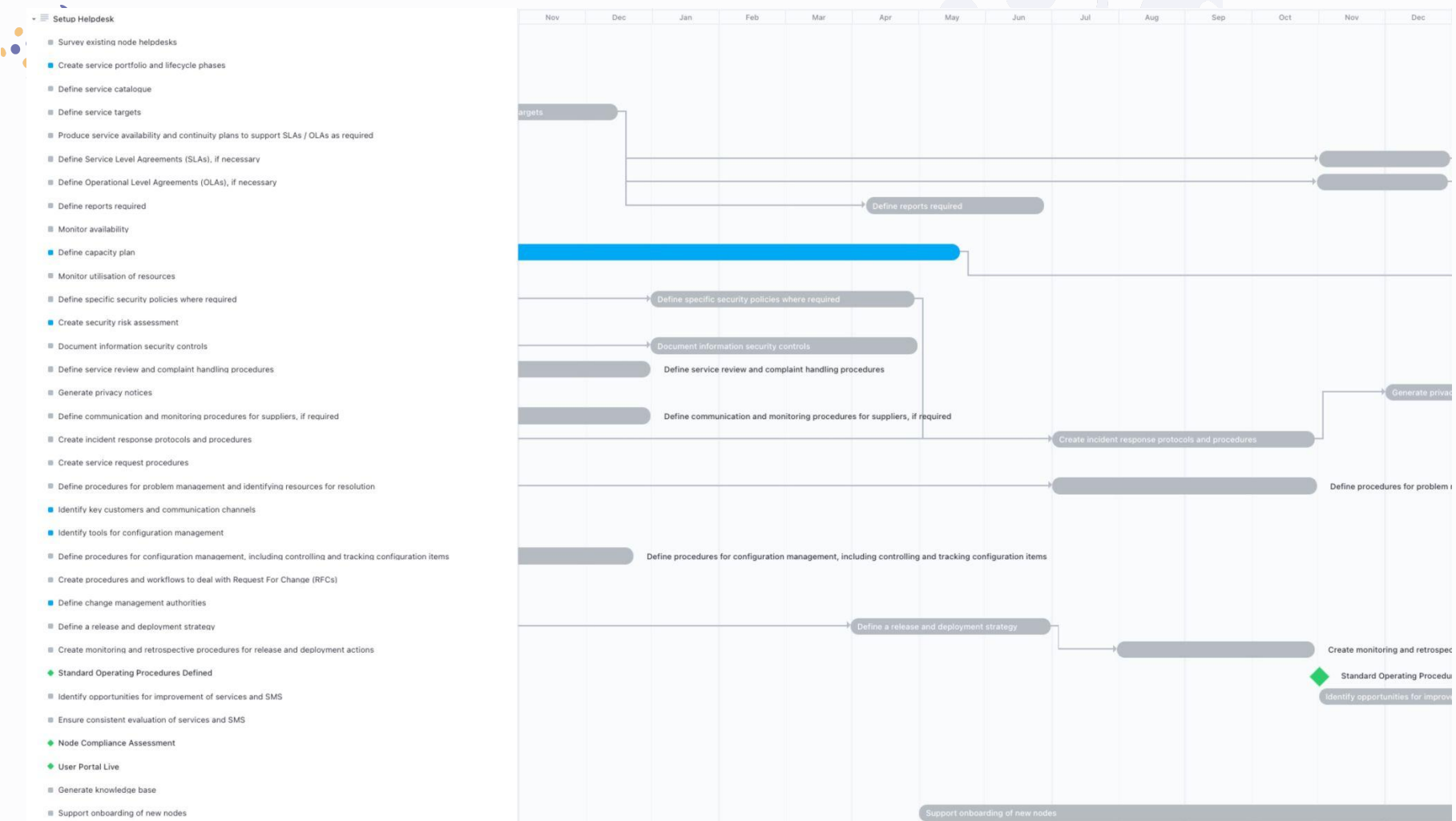**Figure 5**. Gantt chart of the helpdesk roadmap in 2022 to 2023. Blue are tasks in progress as of May 30th 2023.

Figure 6. Gantt chart of the helpdesk roadmap in 2023 to 2024. Blue are tasks in progress as of May 30th 2023.
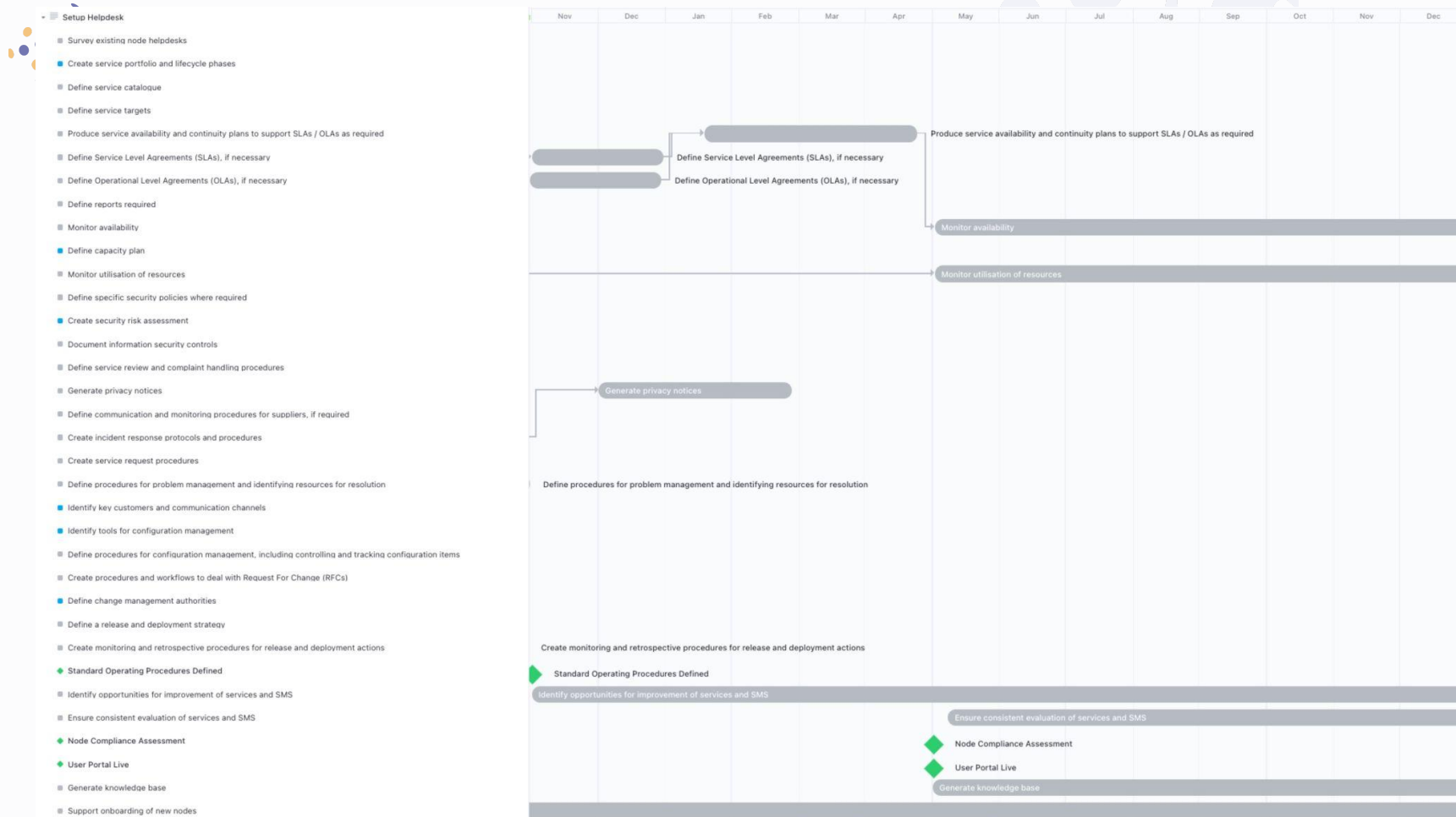
Figure 7. Gantt chart of the helpdesk roadmap in 2024 to 2025.
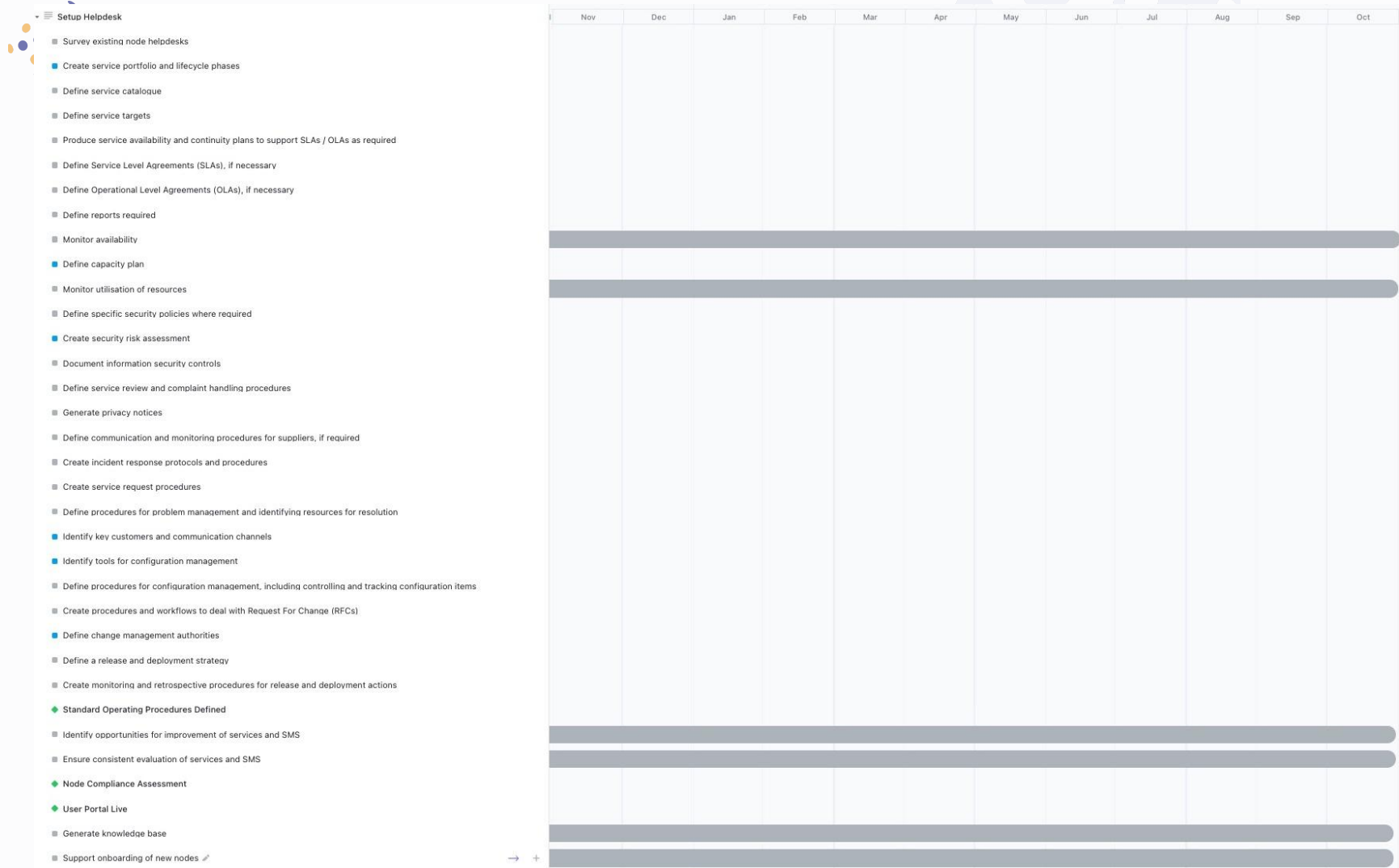
Figure 8. Gantt chart of the helpdesk roadmap in 20225 to 2026.

6. Discussion

As defined in FitSM, standard operating procedures (SOPs) are required to:
- determine how the tickets are distributed, tracked, and responded to.
- distribute development tasks and add these to the roadmap.

External users should have a consistent user experience irrespective of the helpdesk (virtual or node) they are interacting with. This requires SOPs both for the virtual helpdesk, but also for each node. The SOPs will include responses to common queries, procedures to escalate, resolve, or close issues, and classification of issues, and the development of these SOPs are part of Task 4.3 which is due to deliver these by November 2024 as D4.2. To support customer interactions, request tracking, where a request is a communication initiated by a customer to the helpdesk regarding one or more issues, must be defined using clear procedures and policies. There are a range of tools that support helpdesk request tracking, such as RT[10], and interoperability between these tools, where used, must be considered. This will be part of building the service portfolio at the European operations level. Investigating other examples of federated helpdesks, such as LUMI helpdesk[11] run as part of EuroHPC, to determine the best tools to support the federated helpdesk would be run concurrently as part of continual service improvement.

The GDI project has three main use cases as part of Pillar III (Cancer, Infectious Disease, and Genome of Europe) and these use cases can be utilised to help develop the SOPs required to support them over the course of the project. Utilising the use cases as customers while deploying the infrastructure will help develop, expand, and elicit feedback on the helpdesk SOPs during the deployment phase that can then be extended in production with other stakeholders and customers.

Due to the sensitive nature of the data within the GDI, and to ensure that trust is maintained for the wide range of users who are expected to interact with the GDI, a set of robust and unambiguous and well defined SOPs must be created around the data protection and security of the data within the GDI. Some SOPs will be specific to the security of the data within GDI, such as incident or breach response protocols, but all SOPs developed within the GDI must be developed and operated with data protection and security as core values intrinsic to the operation of the GDI.

The GDI project will help support new nodes as they move from on-boarding, through deployment, to operational. The responsibilities between the operational day to day running of the infrastructure, versus the outreach and knowledge transfer, are defined in the Milestone MS10. The Knowledge Base (KB) that will be generated along with the service catalogue will include all the documentation and SOPs utilised within the operation of the GDI, along with higher level material to help knowledge

---

[10] https://github.com/bestpractical/rt
[11] https://lumi-supercomputer.eu/user-support/need-help/

transfer to new nodes. The KB can include the results of the node survey and TRL reporting of nodes at different stages, including their aspiration, to facilitate knowledge transfer and communication of best practice across the GDI. By performing the initial node helpdesk survey, and linking this to the quarterly report, evolving maturity level model (MLM), and GDI roadmap the KB can function as a valuable centralised resource for a range of nodes, customers, and stakeholders.

The SOPs required for the operation of the helpdesk, are part of Task 4.3 will need to be defined and delivered by November 2024 based on the FitSM standard presented here, as well as with feedback from other federated IT service providers, such as Federated EGA. Once the GDI starter kit has been released, it can be used to help develop the service catalogue in collaboration with the vanguard nodes, as well as elicit feedback on the processes and procedures required. It is expected that some pruning of the required processes will be necessary, and this will be done in conjunction with Pillar I where the processes affecting the sustainability and governance of the European GDI are defined.

7. Next steps

The roadmap should be implemented, but also kept under revision similarly to other SOPs, processes, and services as part of continual service improvement. necessary staff members to support these as defined in the FitSM standard.

8. Glossary

Term	Definition
1+MG	1 Plus Million Genome Declaration https://digital-strategy.ec.europa.eu/en/policies/1-million-genomes
activity	Set of actions carried out within a process
configuration items	Element (that can be technical or non-technical) that contributes to one or more service components
ELSI	Ethical, Legal, and Societal Issues
European GDI	The infrastructure deployed as a result of the GDI project
GDI	Genomic Data Infrastructure
GDI project	The Digital Europe grant number which will result in the deployment of the European GDI

GDPR	General Data Protection Regulation
Helpdesk	The individual, group, organisational function or service that a user, customer, or stakeholder interacts with to get help with a problem
policy	Documented set of intentions, expectations, goals, rules and requirements, often formally expressed by top management representatives in an organisation or federation
procedure	Specified set of steps or instructions to be carried out by an individual or team to perform one or more activities of a process
process	Set of activities that bring about a specific objective or set of results from a set of defined inputs.
service	A way to provide value to a user or customer by bringing about results that they want to achieve
service component	Logical part of a service that provides a function enabling or enhancing a service
service management system	Overall management system that controls and supports management of services within an organisation or federation
service provider	Organisation or federation (or part of an organisation or federation) that manages and delivers a service or services to customers
SOP	Standard Operating Procedure
ticket	Document for tracking and logging the process or workflow performed to satisfy the customer