EGI-InSPIRE

EGI OPERATIONS ARCHITECTURE: GRID SERVICE MANAGEMENT BEST PRACTICES

EU DELIVERABLE: D4.3

Document identifier:	EGI-D4.3-v1.3
Date:	**02/12/2011**
Activity:	**SA1**
Lead Partner:	**EGI.eu**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/763

Abstract

The document defines the EGI Operations Service Asset and the related providers and users. It also describes the adopted operations service management best-practices, it analyses the level of conformance to the ITIL stages and processes for IT Service Management, and the existing gaps.



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Tiziana Ferrari	EGI.eu/SA1	26/9/2011
Reviewed by	**Moderator:** S. Andreozzi **Reviewers:** S. Storey, T. Schaaf	EGI.eu Susan Storey Associates LMU	1/12/2011
Approved by	**AMB & PMB**		2/12/2011

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	29/10/2011	v. 1.0	T. Ferrari/EGI.eu
2	23/11/2011	v. 1.1 and v. 1.2 Incorporated changes to address external review comments (S. Newhouse, S. Storey, S. Andreozzi)	T. Ferrari/EGI.eu
3	30/11/2011	v. 1.3 incorporated review comments (T. Schaaf)	T. Ferraro/EGI.eu

IV. APPLICATION AREA

This document is a formal deliverable for the European Commission, applicable to all members of the EGI-InSPIRE project, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGI-InSPIRE "Document Management Procedure" will be followed.
https://wiki.egi.eu/wiki/Procedures

VI. TERMINOLOGY

- **Resource Centre.** The smallest resource administration domain in an e-Infrastructure. It can be either localised or geographically distributed. It provides a minimum set of local or remote IT Services compliant to well-defined IT Capabilities necessary to make resources accessible to Users. Access is granted by exposing common interfaces to Users.
- **Resource infrastructure Provider.** The legal organisation responsible for any matter that concerns the respective Resource Infrastructure. It provides, manages and operates (directly or indirectly) all the operational services required to an agreed level of quality as required by the Resource Centres and their user community. It holds the responsibility of integrating these operational services into EGI in order to enable uniform resource access and sharing for the benefit of their Users. The Resource infrastructure Provider liaises locally with the Resource Centre Operations Managers, and represents the Resource Centres at an international level. Examples of a Resource infrastructure Provider are the European Intergovernmental Research Organisations(EIRO) and the National Grid Initiatives (NGIs).
- **Operations Centre**. A centre offering operations services on behalf of the Resource Infrastructure Provider.
- **EGI.eu.** Organisation based in Amsterdam established to coordinate and manage the infrastructure (EGI) on behalf of its participants: National Grid Initiatives (NGIs) and European Intergovernmental Research Organisations (EIROs).
- **Virtual Organization.** A group of people (e.g. scientists, researchers) with common interests and requirements, who need to work collaboratively and/or share resources (e.g. data, software, expertise, CPU, storage space) regardless of geographical location. They join a VO in order to access resources to meet these needs, after agreeing to a set of rules and Policies that govern their access and security rights (to users, resources and data).
- **Information Technology Infrastructure Library (ITIL).** ITIL ® is a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

The complete EGI Glossary is available at: https://wiki.egi.eu/wiki/Glossary

For acronyms see: http://www.egi.eu/about/glossary/.

VII. PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders.

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting 'Grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop Grids, to benefit user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example within the ESFRI projects. Additional support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today's production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop Grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities (VRCs) − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

VIII. EXECUTIVE SUMMARY

This deliverable provides a high-level description of the Grid service management best practices currently adopted in EGI operations following the ITIL structure of service management service lifecycle covering the following phases: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

The full operations service business catalogue is also defined in this document. EGI operational services are categorized into four groups: Infrastructure and Tools, Grid Services, Support, and Operations and Coordination. Each Service Unit is delivered by a combination of various providers: Resource Centres, Resource infrastructure Providers and EGI.eu, and it provides Local Services (from Resource Centres and Resource infrastructure Providers) and Global Services (from EGI.eu).

The majority of the operational services in the catalogue are targeted to Resource Centres and Resource infrastructure Providers, but some of them are also user-facing such as the Accounting Portal, the MyEGI Portal, the Virtual Organization (VO) management tools and the Service Desk.

The ITIL conformance analysis conducted shows that the set of existing EGI operational processes covers the great majority of the ITIL best practices. The most problematic areas identified concern demand management and capacity management and allocation. While processes exist at a Resource Centre level, EGI as a community is currently missing these processes across multiple providers. These capacity planning and demand planning processes are needed for the effective support of international user communities who do not integrate their own community's resources into EGI. A related process that also needs improvement is the enabling of VO-level access to resources across multiple administration domains (VO access management). It is currently managed and controlled manually, it requires negotiation and agreement with the Resource Centres, and this can introduce delays after a new VO is created when access is highly distributed.

The Service Transition stage has been consolidating during the first year of the process, though the related processes are only applied to Grid services operated by Resource Centres and Resource infrastructure Providers. While for distributed Grid services and tools Service Transition processes were harmonized and indistinctively applied to all production services, a lower level of harmonization is currently present for central EGI.eu Global Services, as in this case Service Transition processes are independently defined and applied by the responsible provider.. This area needs further expansion. In addition, the impact of change after deployment in production is an activity that is currently missing for both Local and Global Services. Impact of change is necessary to assess the quality of new functionality that is delivered with a new deployed software release: testing of new functionality can only be evaluated in a production environment is software clients were also contextually upgraded to make use of it, but this condition is not requested as a pre-requisite for participation to testing activities.

The conformance analysis concentrated on Service Design, Transition, Operation and Continual Service Improvement. As a structural change in the project is being proposed to strengthen strategy planning activities in the EGI ecosystem, the Service Strategy processes were not included in this analysis.

The ITIL conformance study conducted in this deliverable will support future strategy planning activities that concern the analysis of costs, of sustainability and of the business model applicable to the EGI operational services. In addition, the ITIL conformance of operational processes will be periodically reviewed.



TABLE OF CONTENTS

1 INTRODUCTION

This deliverable addresses the following objectives:

- to define the current Catalogue of operational services offered by EGI, and to identify the corresponding groups, the related providers and users;
- to identify the service management best practices currently adopted in EGI operations;
- to verify the level of maturity of EGI operations with regard to the general best practices provided by ITIL, and to perform a gap analysis.

The IT Infrastructure Library (ITIL) defines a best practice framework for the provision of quality IT services, used as the basis for the International Standard ISO/IEC 20000. ITIL aims at defining best practices for the implementation, maintenance and improvement of quality and cost effective IT services. In ITIL a service is a *means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs and risks*. Service Management is the set of specialised organizational capabilities for providing value to customers and users in the form of services.

The ITIL framework is based on five stages of the service lifecycle for service management. This document presents the processes and activities, organization and roles of EGI operations that conform to the ITIL best practices. For each of these stages this document presents the existing best practices adopted by the EGI Operations and identifies those processes that require further development.

The analysis of the current level of conformance of EGI operations to general best-practices, is important to promote the systematic use of service management practices that are responsive, consistent and measurable, to enhance the quality of the services delivered.

This document also presents the EGI Operations Service Asset. The current snapshot of the service catalogue will be used in the coming months to analyse the current consumers of the operational services, value that they provide and the cost of delivering them in order, to understand their routes towards sustainability. This will be undertaken in the context of the strategic plans being developed by the EGI-InSPIRE Project Management Board and reviewed by the EGI Council.

This document is structured as follows. Section 2 presents the operations service groups: Infrastructure and Tools, Grid Services, Support, Operations and Coordination, and the related service providers. Sections 3, 4, 5 and 6 detail the processes currently implemented in EGI Operations in the following four ITIL stages: Service Design, Service Transition, Service Operation and Continual Service Improvement. Finally section 7 draws the conclusions of this work.

2 SERVICE STRATEGY

In the ITIL Service Strategy stage the entire service lifecycle is reviewed to improve service management and tune it according to the business strategy. In Service Strategy objectives and expectation of performance towards serving the customers are defined together with the related priorities. Objectives are implemented through the service lifecycle. The strategy processes are: service portfolio management, demand management and financial management.

Service strategy is at the core of the ITIL Service Lifecycle and defines governance and decision-making and it covers the definition of objectives according to the identified requirements, definition of policies and strategies. All these are reflected in various processes such as financial management, development of offerings, and demand management.

The business strategy for operational services will be started to be addressed as part of the general EGI-InSPIRE strategy planning activities that will take place during PY2. Being the operations business strategy still under discussion, this deliverable does not cover the operations Service Strategy, but rather focuses on the service assets and provisioning mechanisms for the services in the EGI Operations Business Service Catalogue.

2.1 Service Units

In ITIL services are delivered in Service Units, which are bundles of service assets that create value for the customers. Each Service Unit is associated to a Business Unit, i.e. a segment of the business that has its own plans, metrics, income and costs. Each Business Unit owns Assets offered by Service Providers and combined in order to deliver services that create value for Customers.

The overall *Operations Service Asset* includes Local Services – provided by the Resource Infrastructure Provider through their respective Operations Centre – and Global Services – provided by EGI through the coordination of EGI.eu. The Operations Service asset comprehends: *Infrastructure and Tools*, *Grid Services* – release and deployment, *Support* and *Operations and Coordination*. Each unit provides value to a combination of various customer segments (see section 2.3).

2.2 Service Providers

The EGI Operations Service Asset is offered by a combination of three different Service Providers (for definitions of the following terms see section VI).

1. **Resource infrastructure Providers (RPs)**. The Operations Centre is the entity responsible of delivering operations services on behalf of a Resource Infrastructure Provider, and guarantees day-to-day operations management, including support to the associated Resource Centres, the monitoring of performance, the gathering of requirements and their discussion at the EGI Operations Management Board. These services are denominated *Local Services*. "Operations Centres participate at different levels to Service Design, Service Transition, and Service Transition to continuous service improvement. Resource infrastructure Provider responsibilities are described in detail in [RPOLA].
2. **Resource Centres (RCs)**. Resource Centres contribute to the operations management of services that are part of their administration domain, and to their support. These services integrate with the Local Services of the Resource infrastructure Provider, and are part of the same bundle. Resource Centres contribute to strategy planning and policy management in collaboration with their Resource infrastructure Provider. Responsibilities are detailed in [RCOLA].
3. **EGI.eu**. EGI.eu provides central operations and coordination services, and central infrastructure services and tools that are needed for the interworking of those operated locally.

These are denominated *Global Services*. Local and Global Services are complementary and are both necessary for a successful operation of the infrastructure.

The interworking between these three different providers is illustrated in Figure 1.

Figure 1. The EGI Operations Service Assetsincludes Local Services provided by Resource Centres and Resource infrastructure Providers – through their Operations Centres – and Global Services provided by EGI.eu in collaboration with its partners.

2.3 Operations Service Asset

The EGI operations service asset includes four lines of service:

- Infrastructure services and tools (section 2.3.1);
- Grid services: Release and Deployment (section 2.3.2);
- Support services (section 2.3.3);
- Operations and coordination services (section 2.3.4).

For each line the corresponding services are described together with the related providers (EGI.eu, Resource infrastructure Providers, Resource Centres) and the existing users. For each service, the table defines the corresponding ITIL stages and processes the service contributes to implement. The various services in the catalogue are themselves subject to service management processes, however the description of the processes applicable to each individual operational service is out of scope, and is not covered in this deliverable.

2.3.1 Infrastructure and Tools

Table 1. Infrastructure and tools services

Line of service						
Service	**Description**	**Providers (O) = Optional**		**Users**	**Supported ITIL Stages, Processes, Functions**	**Missing features**
		EGI.eu	**RP**			
Message brokers	EGI provides a network of brokers, as a messaging common infrastructure for operational tools	Y		RPs RCs	=	=
Service Availability Monitoring (SAM)	The Monitoring Infrastructure is a distributed service based on Nagios and messaging. The central service include systems such as the MyEGI portal for the visualisation of information, and a set of databases for the persistent storage of information about test results, Availability statistics, monitoring profiles and aggregated topology information. The central services need to interact with the local monitoring infrastructures operated by the RPs.	Y	Y	RPs RCs	**Service Design** (availability management, IT Service continuity management)	RP OLA EGI.eu OLA Availability/Reliability measurement of EGI.eu global services and RP local services
Operations Portal	Central portal for the operations community offers a bundle of different capabilities, such as the broadcast tool, VO management facilities, and a dashboard for Grid operators that is used to display information about failing monitoring probes and to open tickets to the Resource Centres affected. The dashboard also supports the central Grid oversight activities.	Y	Y (O)	RPs RCs	**Service Design** (IT Service continuity management)	EGI.eu core services to be controlled in the Operations Dashboard Failover configuration of EGI.eu technical services
Accounting	The EGI Accounting Infrastructure is distributed. At a central level it includes the repositories for the persistent storage of usage records, and a portal for the visualisation of accounting information. The central databases are populated through individual usage records published by the Resource Centres, or through the publication of summarised usage records.	Y	Y (O)	VRCs RPs RCs	**Service Strategy** (Demand management) **Service Design** (Capacity management)	Storage accounting Grid service accounting
Incident Management Tool (GGUS)	EGI provides support to users and operators through a distributed incident management tool with central coordination (GGUS). This tool provides	Y	Y (O)	VRCs RPs RCs	**Service Operation** (Incident Management, Problem Management) **Service Operation**	=

Line of service					Supported ITIL Stages, Processes, Functions	Missing features
Service	Description	Providers (O) = Optional		Users		
		EGI.eu	RP			
	a single interface for the submission of incident records and requests for change. The central system is interfaced to a variety of other incident management systems at the NGI level in order to allow a bi-directional exchange of incident records.				**Functions:** Service Desk **Service Transition** (Change Management, Service validation and testing)	
Security Monitoring	The objective of Security Monitoring is to protect the Infrastructure from incidents such as exploitable software vulnerabilities, misuse by authorised users, resource "theft", etc., while allowing the information, resources and services to remain accessible and productive for its intended users. Through the coordination groups a specifically designed set of tools and services help reduce these incidents and their impact. These comprise monitoring individual resource centres (based on Nagios and Pakiti); a central security dashboard to allow Resource Centres, NGIs and EGI Computer Security Incident Response Teams (CSIRT) to access security alerts in a controlled manner; and a specific ticketing system to support coordination efforts.	Y	-	RPs RCs	**Service Design** (information security management)	=
Grid Configuration Database (GOCDB)	EGI relies on a central database (GOCDB) to record static information about different entities such as the Operations Centres, the Resource Centres, and the service instances. It also provides contact, role and status information. GOCDB is a source of information for many other operational tools.	Y	Y (O)	VRCs RPs RCs	**Service Design** (Service catalogue), **Service Operation** (Event Management, Problem Management, Incident Management, Request Fulfilment), **Service Transition** (Change, Service Asset Management – People and Infrastructure)	=

2.3.2 Grid Services: Release and Deployment

Table 2. Grid Services

Line of service						
Service	**Description**	**Providers (O) = Optional**		**Users**	**Supported ITIL Stages, Processes, Functions**	**Missing features**
		EGI.eu	**RP/RC**			
Core Grid Services and Catch-all Grid Services	Core Grid services are needed for the authentication of end-users, to allow access to individual RC Grid services, and in some cases to support the running of Infrastructure Services. Examples of such services are VOMS, VO management of infrastructure VOs (DTEAM, OPS); the provisioning of middleware services needed by the monitoring infrastructure (e.g. top-BDII and WMS); the catch-all CA; and other catch-all core Grid services to support small user communities (central catalogues, workflow schedulers, authentication services).	Y	Y	VRCs RPs	**Service Operation** (Function: IT Operations Management)	=
Interoperability	Analysis of interoperability problems when new technologies are being integrated to make sure that new resources and services are measured and compared to targets, to ensure usage and performance are monitored, registered etc. EGI.eu provides the coordination of these activities.	Y	Y (O)	RPs	**Service Design** (Design Coordination)	=
Staged Rollout	Deployed software updates need to be gradually adopted in production after internal verification. This process is implemented in EGI through staged rollout, i.e. through the incremental deployment of a new component by a selected list of candidate Resource Centres.	Y	Y (RCs)	RPs RCs	**Service Transition** (Release Deployment and Management)	Central operational tools are not subject to staged rollout
Requirements Gathering	Production of a Statement of Requirements	Y	Y	RPs RCs	**Service Design**	=
Requests for Changes	The Service Desk processes Request For Changes that are escalated to the appropriate technology provider	Y		RCs RPs EGI.eu	**Service Transition** (Change Management)	

2.3.3 Support Services

Table 3. Support Services

Line of service							
Service	**Description**	**Providers (O) = Optional**			**Users**	**Supported ITIL Stages, Processes and Functions**	**Missing features**
		EGI.eu	**RP**	**Technology Provider**			
1st level support	Incident and problem records that are submitted centrally through the EGI Service Desk are handled internally and are escalated to 2nd level support in case they require specialized support (Provider: EGI.eu) Incident and problem records can be also submitted locally to the local Service Desk operated by the Resource Centre and/or the Resource infrastructure Provider. Local tickets will be escalated to the Resource infrastructure Provider or the EGI.eu 2nd level support units if specialized support about deployed software is required (Provider: RC/RP) Through the EGI incident management tool (GGUS) incident records are routed through to NGI support teams. Some of these records may be related to specific support units but others issues relating to users' use of the e-infrastructure will require human intervention either from an operational or user support aspect.	Y	Y		RPs RCs VRCs EGI.eu	**Service Operation** (Incident management, Problem management)	=
2nd and 3rd level support	An incident can affect a specific Resource Infrastructure, in which case an Incident Record is forwarded to the Resource infrastructure Provider Service Desk for 2nd level support (Provider: RP). Also, 1st level support may be unable to resolve an incident. In all these cases 2nd line support is needed to implement incident escalation. Incident management indicates that the root cause of the incident is one or more problems. The 2nd level Support Units of the EGI.eu Service Desk are then contacted (Provider: EGI.eu). 3rd level support units are also available. 3rd level support groups can be internal (for the operational tools developed in EGI-InSPIRE) or a third party (the external technology providers).	Y	Y	Y	RPs RCs VRCs EGI.eu	**Service Operation** (Incident management, Problem management)	=
Early Life Support	A selected list of expert RCs participate to the early adoption of new software releases. Incidents experienced during this phase are recorded by the early adopters and handled by the EGI Service Desk. These incidents are directly escalated to the technology providers. EGI.eu is responsible of coordinating this process.	Y			RCs	**Service Transition** (Service validation and testing)	=

2.3.4 Operations and Coordination

Table 4. Operations and Coordination

Line of service					Supported ITIL Stages, Processes and Functions	Missing features
Service	Description	Providers (O) = Optional		Users		
		EGI.eu	RP			
Grid oversight (COD, ROD, RC)	Grid operations oversight activities include the detection and coordination of the diagnosis of problems affecting EGI until their resolution. The daily operation of the infrastructure at RC, RP and EGI.eu level	Y	Y	RPs RCs EGI.eu	**Service Operation** (Event Management) Function: IT Operations Management **Service Transition** (knowledge management – ROD Newsletter)	=
Operations Coordination	Monitoring of status of capacity utilization, planning of expansion (EGI.eu, RPs, RCs) Policy management, strategy planning (EGI.eu, RPs, RCs) Security coordination: Security vulnerabilities and risks presented by e-Infrastructures provide a rationale for coordination amongst the EGI participants at various levels. Central coordination groups are involved in policy development and coordination operational security (EGI.eu, RPs). Coordination of staged rollout (EGI.eu) Coordination of interoperation (EGI.eu)	Y	Y	RPs RCs EGI.eu	**Service Design** (capacity management and Planning) **Service Transition** (Transition Planning and Support) **Continual Service Improvement**	Coordinated capacity management and Planning across multiple providers
Availability management	Overseeing of Availability status of services and support at RP and EGI.eu level (EGI.eu and RPs), and comparison with defined service targets	Y	Y	RPs RCs EGI.eu	**Service Design** (availability management)	
Service Level Management	Supervision of performance measurement and report generation, verification and distribution of monthly Availability reports (Resource Centre and Resource infrastructure Provider reports), modification of reports in case of problems with the tool infrastructure (EGI.eu) Definition of roles, responsibilities and maintenance of the procedures for handling of procedures for report management (EGI.eu)	Y	Y	RPs EGI.eu	**Service Design** (Service Level Management)	

Line of service					Supported ITIL Stages, Processes and Functions	Missing features
Service	Description	Providers (O) = Optional		Users		
		EGI.eu	RP			
Security Management	Vulnerability and risk assessment, incident response, security coordination and support, assessment, training. These concern both the services provided locally by RPs and centrally by EGI.eu	Y	Y	RCs RPs EGI.eu	**Service Design** (Security Management) **Service Transition** (Knowledge Management)	
Documentation	Maintenance and development of operational documentation, procedures, best practices, etc. EGI.eu provides Technical Coordination of this community activity, and connects partners with specialized expertise.	Y	Y	RPs RCs	**Service Transition** (knowledge management)	

3 SERVICE DESIGN

In this stage the plans produced by the service strategy are translated into the blueprint for delivering the related objectives [IT-D]. During service design strategic principles are converted into a service portfolio. Service design not only concerns new services but also services that are already part of the service portfolio. Changes and improvements can be necessary to maintain or enhance or maintain the value to customers.

Service design is structured as a set of activities and/or processes that are needed to identify requirements and define the proposed solution that is able to meet these requirements.

3.1 Design co-ordination

Design co-ordination is the activity or process that identifies requirements and then defines a solution that is able to meet these requirements [REQ].

Requirements about the deployed technology and operational tools are periodically collected from Resource Centres and Resource infrastructure Providers. Requirements about Grid deployed technology are discussed and prioritized in the framework of the Operations Management Board [OMB]. Those which are approved are handled to the technology providers, and if critical or controversial are taken for discussion with the Technology Providers of EGI to the Technology Coordination Board [TCB].

Requirements that concern tools follow a similar process with the difference that these are initially discussed and prioritized in the framework of a dedicated board: the Operational Tools Advisory Board [OTAG].

Requirements that concern areas other than software, such as documentation, procedures, policies etc. are discussed at the Operations Management Board.

The overall process is illustrated in Figure 2. The resulting statement of requirements is available at [SOR].

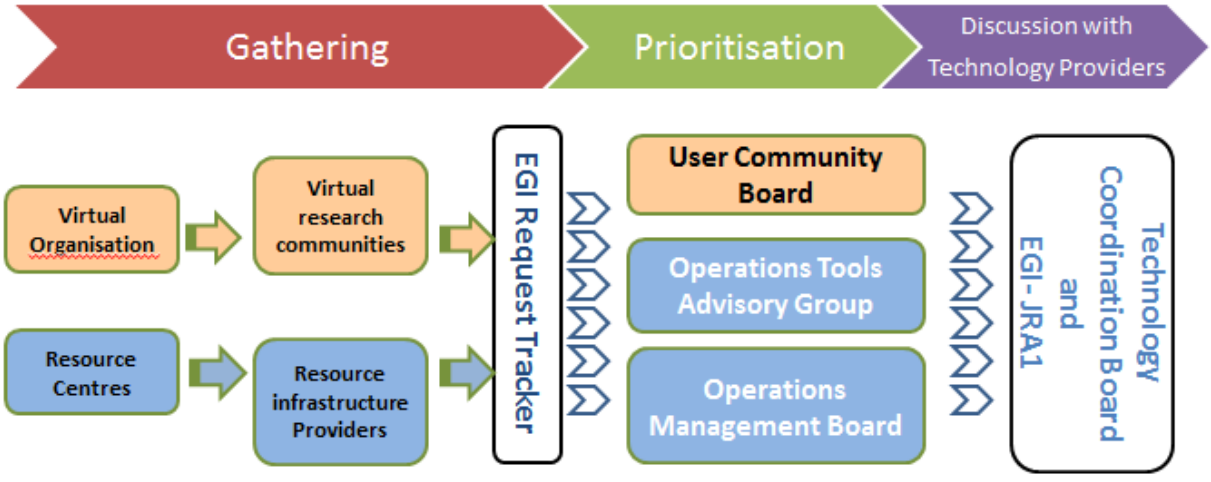

Figure 2. Requirements gathering process (blue rectangles) supporting design coordination at the Technology Coordination Board.

3.2 Service catalogue management

The service catalogue is a database or structured document with information about all live IT services, including those available for deployment. The service catalogue is the only part of the service portfolio published to customers (which is owned by the service strategy stage), and is used to support the sale and delivery of IT Services. When service strategy charters a service, the commitment to deliver something in the pipeline is articulated through an entry in the Service Catalogue, which includes expected functionality and delivery date, information about deliverables, prices, contact points, ordering and request processes.

On the other hand, the business service catalogue contains details of all the IT services delivered to the customer, together with relationships to providers and customers.

Resources and Grid services either operated by Resource Centres or by EGI.eu are registered in the EGI repository for storing and presenting topology and resource information, named GOCDB[1].

GOCDB provides information about production services and information about the respective administrators and security contacts. It also supports service management functions such as declaring a downtime.

3.3 Service level management

Service level management is the process responsible for negotiating service level agreements, and ensuring that these are met. It is responsible for ensuring that all IT service management processes, Operational Level Agreements and underpinning contracts are appropriate for the agreed service level targets levels, and holds regular customer reviews.

EGI Operational services that are facing internal operational entities are regulated by Operational Level Agreements (OLAs).

1. The Resource Centre OLA [RCOLA] was formalized in May 2011, and its acceptance is a pre-requisite for a Resource Centre to be part of the production infrastructure [PROC09].
2. The Resource infrastructure Provider OLA was approved in October 2011, and its acceptance is a pre-requisite for a Resource infrastructure Provider to be part of EGI regardless of the Resource infrastructure Provider status.

The Operational Level Agreement framework will be extended to include an EGI.eu OLA addressing the EGI.eu Global Services.

OLAs are binding Resource Centres and Resource infrastructure Providers that are either EGI participants (i.e. are members of the EGI Council) or integrated Resource infrastructure Providers – these make use of EGI operational services without being part of the EGI governance structure [ARC]. In the latter case, OLAs are negotiated in the framework of a Resource Infrastructure Provider MoU [MOU]. Two MoUs have been approved since the beginning of EGI-InSPIRE: one with Iniciativa de Grid de America Latina [IGALC] and a second one with the South African Grid Initiative [SAG].

Service target levels (Availability and Reliability – see section **Error! Reference source not found.**) re monitored and reports are generated on a monthly basis. These are accessible at [PERF]. Underperforming Resource Centres are those who delivered less that 70% monthly Availability. These are contacted to conduct a post-mortem analysis of the problems experienced. In case of prolonged low Availability (three consecutive calendar months), underperforming Resource Centres are suspended. This procedure for internal quality verification is documented at [PERF].

[1] https://goc.egi.eu/portal/

A procedure is also available to collect feedback from the Resource Centres in case of wrong measurements that affected Availability and Reliability reports [PROC10]. In case of errors, Availability and Reliability reports are recomputed and distributed to the stakeholders.

3.4 Capacity management

Capacity management is the process responsible for ensuring that the capacity of IT services and the IT infrastructure is able to deliver agreed service level targets in a cost effective and timely manner. Capacity management considers all resources required to deliver the IT Service, and plans for short-, medium- and long-term business requirements.

In EGI, the capacity management process is applied to resources (computing, storage and networking) and the Grid interfaces used to provide access to them (Computing Element layer, Storage Element layer and the collective Grid middleware services such as VOMS for user authentication, WMS and FTS for compute and data transfer job scheduling, the Information Discovery System, etc.).

- **Resource accounting.** Accounting for resource usage is implemented through the EGI accounting infrastructure: a distributed system consisting of probes extracting usage records from resources at the Resource Centre level, and of repositories and portals providing aggregation of usage records at different levels (Resource Centre, Resource infrastructure Provider and EGI for an overall view of resource utilization across the integrated infrastructure). The accounting infrastructure is currently capable of collecting information about usage of compute resources. Plans are being defined in collaboration with the EGI technology providers to extend this framework to data storage and other types of integrated resources.

  The Accounting Portal[2] it the tool responsible of providing access to accounting data. The portal provides different types of views at different levels: user views, VO-specific views, and aggregated views per Resource Centre, per Operations Centre and for the whole EGI infrastructure. In VO-specific view (for example the WLCG reports), utilization is compared to installed capacity to get information about percentage of utilization and compute job efficiency[3].

- **Grid service accounting**. EGI is currently not performing accounting of Grid services providing access to individual resources. Capacity management for these services is currently performed by Resource Centre administrators and/or Operations Centres operators by using local tools, which measure a range of service status parameters such as load, status of queues, disk and memory utilization etc. The implementation of a harmonized Grid service status monitoring framework is being investigated by the European Middleware Initiative – EMI [EMI] as part of the Infrastructure Area work plan [MON], and will be evaluated for deployment in EGI.

The entities responsible of capacity management are:

- The Resource Centre administrators for the resources and Grid services operated in their administration domain.
- The Resource infrastructure Providers for the Grid services and operational infrastructures and tools under their operational responsibilities.
- The partners of EGI.eu that technically deliver the EGI.eu Global services and tools.

[2] http://accounting.egi.eu/

[3] For a user-specific accounting view see for example the WLCG Tier2 accounting reports at http://accounting.egi.eu/Gridsite/accounting/CESGA/reptier2.html.

The accounting portals provide either centrally at EGI level or locally at Resource infrastructure Provider level, information about usage or resources (currently computing resources) through different view:

- User aggregation:
  - per individual end-user,
  - per Virtual Organization (VO),
  - per scientific discipline.
- Infrastructure aggregation:
  - per Resource Centre,
  - per Resource Infrastructure Provider,
  - EGI.

Usage records are collected locally and aggregated centrally. The accounting portal shows usage patterns, and compares the distribution of utilization across the infrastructure and across different end-user communities. Currently no pricing is associated to utilization. In the future, accounting information will assist providers with the definition of pricing mechanisms for the portfolio of EGI services.

Gap analysis: Whilst activities and roles are well identified at various infrastructure layers (resource Centres, Resource infrastructure Provider services, EGI.eu services), roles and procedures are missing for a coordinated capacity management and planning across the various providers.

3.5 Availability management

Availability management is the process responsible for defining, analysing, planning, measuring and improving all aspects of the Availability of IT services. Availability management is responsible for ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed service level targets for Availability.

EGI defines the following level targets [ACE]:

- **Availability** of a service instance, service or a site over a given period is defined as the fraction of time the same was in the *UP Period* during the known interval in the given period. The *UP Period* is defined to be the period over which the status of the entity was either OK (the service, service flavour or RC is working) or WARNING (the service, service flavour or site is working, but with non-critical alarms) and the entity was not in scheduled downtime. For Availability, computation status WARNING is considered as good as OK.
- **Reliability** of a service instance, service or a site over a given period is defined as the ratio of the time interval it was in the *UP Period* over the time interval it was supposed (scheduled) to be UP during the known interval in the given period.

Service level targets are defined in the Resource Centre Operational Level Agreement [RCOLA] and in the Resource infrastructure Provider Operational Level Agreement [RPOLA].

SAM provides the central MyEGI component[4] which is the availability management Information System of EGI, where both Availability and Reliability data can be accessed at different aggregation levels: per technical services, per Resource Centre and per Operations Centre.

Availability and Reliability reports are generated, validated and distributed centrally by EGI.eu through its technical partners, and EGI.eu holds the ownership and the management of the related roles and processes. The monitoring of performance, the overseeing of the overall infrastructure status are distributed activities: the Operations Centres are responsible for their national/federated local

[4] https://Grid-monitoring.cern.ch/myegi/

infrastructure, while the COD team of EGI is responsible of monitoring the quality delivered by the Resource infrastructure Providers and of oversight activities.

Problems with the reported performance can be notified to the service desk (a dedicated support unit is available).

3.6 IT service continuity management

IT service continuity management is the process responsible for managing risks that could seriously affect IT services, and it ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services.

Continuity of Grid middleware services is proactively monitored through the Operations Dashboard[5] provided by the Operations Portal. In the dashboard alarms are displayed when an OPERATIONAL test fails. Failure is promptly notified to the administrators of the service. Currently, not all Global services are under dashboard monitoring as the framework is being extended. Purpose of this process is to:

- **Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets**. Several operational functions are distributed across several teams. The operational supervision of the Operations Centre is allocated to two teams that are involved in rota in order to improve time coverage. Similarly, ticket triage is distributed across two teams of shifters.
- **Ensure that proactive measures to improve the Availability of services are implemented wherever it is cost-justifiable to do so.** In order to improve the robustness of Grid middleware services, failover and/or high availability configurations are deployed locally or requiring geographical distribution. The deployment of these configurations is promoted by EGI, its adoption is however under the responsibility of the Resource Centre administrators. Currently, not all EGI.eu Global Services are in failover/high-availability configuration: this is being improved. EGI is developing manuals providing guidelines about the failover deployment of core Grid middleware services.
- **Risk analysis (RA)** includes risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified. EGI-InSPIRE will perform a risk assessment activity during PY2; the plan and process will be documented in deliverable D4.4.

3.7 Information security management

Information security management is the process that ensures the confidentiality, integrity and Availability of organization assets, information, data and IT Services. EGI adopts an information security management system that comprises:

- **Security Policies**: these are publicly accessible[6] and periodically updated. The process for the development and approval of security policies is under the responsibility of the Security Policy Group. The process is documented in [MS209].
- **Security Procedures**: these are adopted to provide guidelines for security incident handling, vulnerability issue handling, and critical vulnerability operational handling. Procedures are approved following the EGI Policy Decision Process and are publicly available at [SEC].

[5] https://operations-portal.egi.eu/dashboard
[6] https://wiki.egi.eu/wiki/SPG:Documents

- **Tools** for the monitoring of the security level of the infrastructure and for the identification of security operational issues in the Security Dashboard are available to support daily proactive monitoring:
    - Pakiti[7] is a client-server tool that collects and evaluates data about packages installed on Linux machines, primarily meant to identify vulnerable software packages that have not been properly updated. The EGI CSIRT operates the EGI Pakiti instance that is used to monitor the state of the EGI sites.
    - Security monitoring system with Nagios
    - Security Dashboard (being prototyped)
    - Dedicated ticketing system to maintain confidentiality on open issues.

Information security management is structured through various boards:

- **EuGridPMA**: the European Policy Management Authority for Grid Authentication and the International Grid Trust Federation - IGTF at the global level, coordinate the trust fabric for e-Science authentication in Europe. EUGridPMA establish common policies and guidelines for authentication management authorities that provide identity assertions to people, network systems and services for use in the e-Infrastructure. Participation by EGI and EGI-InSPIRE in sustaining and evolving the global trust fabric ensures continued interoperability, both at the European as well as the global scale, and it will aid the adoption of EGI authentication and security requirements at the global level. EGI has joined the EUGridPMA as a Relying Party member on June 16th, 2010 [MS208].
- **Software Vulnerability Group** and the **Risk Assessment Team**. The main purpose of the Software Vulnerabilities Group (SVG) is to manage vulnerabilities observed within the deployed infrastructure, primarily from the Grid middleware developed specifically for EGI, prevent the introduction of new vulnerabilities from the use of 3rd party software packages and to prevent security incidents. In addition, some of the specific activities include software vulnerability issue handling, vulnerability assessment, vulnerability prevention etc. The EGI Risk Assessment Team is the group of people who carry out most of the work to investigate and assess vulnerabilities reported to the EGI Software Vulnerability Issue handling process.
- **Computer Security Incident Response Team**: CSIRT will advise and recommend on security matters and have the power to suspend sites from the infrastructure if they fail to apply critical security patches. The EGI CSIRT ensures both the coordination with peer Grids and with the NGIs and NREN CSIRTs. The EGI CSIRT acts as a forum to combine efforts and resources from the Resource infrastructure Providers in different areas, including Grid security monitoring, Security training and dissemination, and improvements in responses to incidents.
- **Incident Response Task Force:** handles day to day operational security issues and coordinate Computer-Security-Incident-Response across the EGI infrastructure.
- **Security Policy Group:** is charged with developing and maintaining Security Policy for use by EGI and the NGIs. This EGI Security Policy defines the expected behaviour of NGIs, Sites, Users and other participants, required to facilitate the operation of a secure and trustworthy distributed computing infrastructure. SPG may also provide policy advice on any security matter related to the operation of the EGI infrastructure.
- **Security Coordination Group**: brings together representatives of the various security functions within the EGI to ensure that there is coordination between the operational security, the security policy governing the use of the production infrastructure and the technology providers whose software is used within the production infrastructure[8].

[7] http://pakiti.sourceforge.net/

[8] https://documents.egi.eu/document/119

3.8 Supplier management

The supplier management process ensures that suppliers and the services they provide are managed to support IT service targets and business expectations.

This process currently just includes two activities related to EGI.eu Global Services that are outsourced to Resource infrastructure Providers.

- Manage relationships with suppliers: providers of EGI.eu Global Services were initially identified through a bidding process during the preparation phase of the EGI-InSPIRE project. These providers are contractually bound by the EGI-InSPIRE grant agreement.
- Manage supplier performance: technical Global Services are periodically monitored, but no Operational Level Agreement is currently in place for those, and the related Service Target levels have still to be defined. Both activities are part of the PY2 roadmap of EGI-InSPIRE.

Gap Analysis: This process requires further development in EGI.

4 SERVICE TRANSITION

This stage defines the processes needed for the development and improvement of new capabilities. The processes transform the requirements defined during the service strategy and implemented in service design, into service operation while managing the risks related to the changes introduced by the transition itself [IT-T].

EGI service transition comprehends:

- Evolve the Grid capabilities to fix problems affecting the deployed services;
- Evolve the Grid capabilities to made new functionality that is released by the Technology Providers available to the end-users;
- Plan and manage the capacity and resources needed for an incremental staged deployment of new capabilities;
- Plan for new releases (frequency and timing);
- Technically evaluate new releases according to their relevance to the community through the initial validation in a small-scale testbed for the verification of the quality criteria defined during Service Design;
- Technically evaluate in collaboration with expert Resource Centre the scalability and Availability of service updates by exposing them to production configurations and end-user worflows;
- Monitor the technology support calendars, negotiate changes and decommission unsupported services;
- Define the tools and workflows to collect feedback from validators and staged rollout Resource Centres, and to communicate results to the Technology Providers;
- Document problems and workarounds defined during validation and staged rollout and document these in release notes;
- Coordinate the various activities herein identified.

4.1 Transition planning and support

Transition planning and support is the process that is responsible for planning all service transition processes and coordinating the resources that they require. These processes are: change management, service asset and configuration management, release and deployment management, service validation and testing, evaluation and knowledge management (see following sections).

EGI transition planning activities comprise:

- Plan capacity and resources that are provided by the Resource Centres through the coordination of the Resource infrastructure Provider, to participate to staged rollout (EGI.eu responsibility)
- Plan the large-scale adoption of new software that is ready for deployment (EGI.eu responsibility) and establish the new services in production (EGI.eu, RP or RC responsibility depending on the type of service).
- Plan capacity and resources to release new services (EGI.eu responsibility). This includes a software repository, the operation of a news feed for announcement of new releases, a request tracker to support the service verification and testing processes, and web pages to document new releases[9].

[9] This activity is reported here for completeness but is under the technical responsibility of EGI-InSPIRE SA2.

- Ensure that incidents emerged during service testing and the related risks are assessed by the appropriate bodies such as the Operations Management Board and the User Community Board (EGI.eu responsibility).
- Coordinate the teams participating to staged rollout (EGI.eu responsibility).

Gap analysis: Transition planning and support is currently applied to RC and RP services that are deployed at large scale. On the other hand, transition of EGI.eu services is not subject to structured planning. This process needs to be extended to EGI's Global Services to ensure quality of service during transition.

4.2 Change management

Change management has responsibility for ensuring that changes are accurately assessed for risk and managed accordingly to minimise disruption. This implies an oversight role to make sure that changes are properly tested and according to the timelines provided to the Early Adopters. The change management responsibility in the operations area is assigned to EGI.eu and technically run by an EGI-InSPIRE partner (the change manager).

In addition to backing support activities, GGUS is also used to record Requests For Changes (RFCs). These are negotiated with the technology providers. In addition, GGUS is also used to communicate incidents and problems affecting the newly released technology, as a result of validation and testing.

The change advisory board supports the authorization of changes and assists change management in the assessment and prioritization of changes. The change advisory board function is constituted by the Operations Management Board, the team of Early Adopters involved in the testing and the change manager. In case of changes that have an impact on end-user activities, the EGI User Community Board is involved too.

EGI is currently not engaged in change review activities to check that enhancements, bug fixes and new features introduced are functionally correctly delivered. This area will be explored as potential extension of the current Staged Rollout activity.

Procedures for change management are customized in case of an emergency change, which is defined as a change that must be introduced as soon as possible. For example, to resolve a Major Incident or implement a Security patch. In case a critical vulnerability is identified, the Critical Vulnerability Operational Procedure [SEC03] is applied. According to this procedure, after a problem has been assessed as critical, and a solution is available, then Resource Centres are required to take action. Procedure SEC03 primarily defines the procedure from this time, where Resource Centres are asked to take action, and what steps are taken if they do not respond or do not take action. If a Resource Centre fails to take action, this may lead to site suspension. In addition, in case of release of an emergency fix, a modified Staged Rollout procedure is adopted ensuring that after release in one business date the change can be approved or rejected.

4.3 Service asset and configuration management

Assets of a service provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure and financial capital. The asset register is the list that includes information about *ownership* and *value*. Asset management maintains the asset register.

- **Management**: management is a system that includes leadership, administration, policies, performance measures and incentives. This layer cultivates, coordinates and controls all other asset types. EGI service asset management in this specific area is limited to the recording of EGI policies (wiki and Document DB) [POL], and of policy bodies agendas and actions (managed through on the on-line agenda management system if EGI).

- **Organization**: information about existing operational teams and boards, and the management of the related membership, are supported by the EGI Single Sign On system[10]
- **Process**: processes are structured sets of activities, and activities are structured as set of steps documented in procedures. EGI Operational Procedures (operational and security-related) are available on-line of wiki or the EGI Document DB [PROC], and the current level of comprehensiveness of activity documentation is good. However, documentation of EGI processes is probably an area which requires more development.
- **People**: operational contact information and people roles are documented and managed through GOCDB [GOC].
- **Information**: Information assets are collections, patterns and meaningful abstractions of data applied to various areas such as operations. Operational information is collected and maintained primarily through – in order of importance: the EGI Operations wiki, the EGI Document DB, and the EGI web site[11].
- **Applications:** user community applications that were ported to Grid are recorded in the EGI central application database [ADB].
- **Infrastructure:**
  - Service end-points are recorded in GOCDB [GOC]. Dynamic status information of Grid services – including information about software release and version - is accessible through the EGI Information Discovery system (currently covering gLite resources, but not ARC and UNICORE) [EMI].
  - No central information is available about the fabric-layer of the infrastructure (network, batch system, etc.). This is handled locally by Resource Centres.

Configuration management is the process responsible for maintaining information about the configuration items required to deliver an IT Service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management. Configuration item characteristics are described in documents that cover aspects such as service definition, requirements specification and service level agreement for a service, and relationship with other items such as "is part of", "is connected to", "uses", "is installed on" etc.

Gap analysis: GOCDB provides only a very limited set of Configuration Management System features, and just limited to Grid software assets. This process requires further development in EGI.

4.4 Release and deployment management

Software updates need to be gradually adopted in production after internal verification. This process is implemented in EGI through staged rollout, i.e. through the early deployment of a new component by a selected list of candidate Resource Centres.

Service deployment follows a pull approach as Resource Centre administrators are free to upgrade following the local maintenance schedule, in agreement with the VOs that are locally supported. This is generally applicable with the exception of critical vulnerability, in which case a software upgrade can be requested within seven calendar days [SEC03].

4.5 Service validation and testing

In EGI deployed software updates need to be gradually adopted in production after internal verification. This process is implemented in EGI through staged rollout [SRW] [MS409], i.e. through the early deployment of a new component by a selected list of candidate Resource Centres. The

[10] https://www.egi.eu/sso/
[11] https://wiki.egi.eu/wiki/Operations, https://documents.egi.eu/public/DocumentDatabase, http://www.egi.eu/

successful verification of a new component in a production environment is a precondition for declaring the software ready for deployment. Given the scale of EGI, this process requires careful coordination to ensure that every new capability is verified by a representative pool of candidate Resource Centres. The responsiveness of the Resource Centres needs to be supervised to ensure that the staged rollout progresses well without introducing unnecessary delays, and to review the reports produced. It also ensures the planning of resources according to the foreseen release schedules from the Technology Providers. EGI.eu coordination is necessary to ensure a successful interoperation of the various stakeholders: Resource Centres, Technology Providers, the EGI.eu Technical Manager and the EGI Repository Managers.

4.6 Change evaluation

The Early Adopter Resource Centres that participate to the installation of a new Grid service release are independent assessors of the impact of the change. Approval, rejection or approval with workarounds to a given upgrade is formally documented through a staged rollout report [SRT].

The change authority is represented by the group of Resource Centres that are involved in the Staged Rollout of a given capability. Collectively these evaluate the change based on impact, urgency, risk and benefits. In some cases assessment can be controversial, as problems may be discovered by a subset of the assessors, or assessed problems may have a different impact on different user communities. In such cases of uncertainty, the assessment problem is escalated and the operations community – together with the Early Adopters – is invited to decide and provide a change authorization.

4.7 Knowledge management

Knowledge management is the process responsible for gathering, analysing, storing and sharing knowledge and information within an organization. The primary purpose of Knowledge management is to improve efficiency by reducing the need to rediscover knowledge.

Knowledge is managed in various areas and is technically maintained by the community, which comprises: Resource infrastructure Provider experts, Resource Centre experts and EGI.eu. Knowledge is conveyed by different means:

- EGI wiki: to provide access to Operational procedures, manuals, best practices, how-TOs, FAQs and troubleshooting guides [DOC].
- Newsletters: to keep Regional Operators on Duty informed about recent developments [ROD]. The Newsletter is an effective communication means as Grid oversight activities are carried out by a geographically distributed large team.
- Press articles: to inform the general public about the operations status and accomplishments [PRE].
- News feeds: to communicate about technical changes relevant to the infrastructure operation [NEWS].
- Training: technical knowledge is delivered by Resource infrastructure Providers through training events, whose material can be shared through the Training Market Place [TPM]

EGI.eu provides the coordination part of knowledge management activities. This includes the periodic review of the existing knowledge base.

Gap analysis: Because of the highly distributed nature of the teams involved in the operations of the infrastructure and the large amount of knowledge available in various forms, management of the existing knowledge base is currently not formally structured, and in particular it is not tightly coordinated with other service areas of EGI. Examples of activities that need to be strengthened are:

status assessment, lifecycle management, assessment of impact of existing document, analysis of knowledge demand.

5 SERVICE OPERATION

Service operations is the stage that provides guidance on how to **maintain stability** in service operations, allowing for changes in design, scale, scope and service levels. Processes and tools are put into place for reactive and proactive control [IT-O].

5.1 Improvement of operational activities

EGI Operations have been engaged in a number of activities to improve the performance and cost in several areas:

- **Automation of manual tasks:** follow up of event notifications is a human labour intensive activity that has been simplified through the operations dashboard, which allows the creation of incident records when critical conditions arise. In addition, given the scale of EGI controlling monthly service reports is time consuming, so we are seeking for mechanisms that allow the automatic generation of event notifications when performance is not respecting the service targets defined in the relevant Operational Level Agreements. In addition, we are working towards the unification of various escalation processes unifying incident escalation workflows for operational and non-critical security problems.
- **Operational audits:** EGI operational services (central and local) are audited on a yearly basis. This includes the auditing of the performance of the service desk and of incident management activities. Procedures and documentation are periodically reviewed. Performance of the Grid services operated by the Resource Centre administrators and by the Resource infrastructure Providers are audited every month.
- **Communication:** communication between teams responsible for design, support and operation of services is ensured by various means:
  - targeted broadcast messages[12] that can be directed to Resource Centre administrators, Operations Centres, Operations management, and VO managers;
  - Mailing lists and blog posting.
- **Education and training**: training events are co-located with major community events. Material from local training events is shared through the training market place [TMP].

5.2 Event management

Event management is the process that *monitors* all events that occur through the IT infrastructure to allow for normal operation and also to detect and escalate exception conditions. An event is defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT services. Event management is at the basis of operational control and monitoring.

Effective service operation is dependent on knowing the status of the infrastructure and detecting any deviation from normal or expected operation. This is provided by the Service Availability Monitoring system and by the operations dashboard (see section 2). SAM is an active monitoring tool that polls status and Availability of Resource Centre services. Exceptions (i.e. failures of operational tests) will generate an alert that is communicated to the operations dashboard. Resource infrastructure Provider failures are notified to the respective operations team. Passive monitoring of status is typically used locally at Resource Centres to monitor local infrastructure services.

Grid operations oversight activities include the detection and coordination of the diagnosis of problems affecting EGI until their resolution. It includes the reporting of middleware issues to the

[12] https://operations-portal.egi.eu/broadcast

developers, the execution of quality checks of the services provided by Resource infrastructure Providers, and the handling of operational problems that cannot be solved locally. Oversight activities take place locally within each Operations Centre as well as to coordinate the oversight of the national e-Infrastructures.

Notifications are based on *alert and human intervention*. Alerts that are not handled in a timely fashion by the Regional Operator on Duty – ROD – teams are escalated to the central one (Central Operator on Duty – COD).

ROD activities include monitoring of the services operated by Resource Centres, the management of tickets and their follow up for problem resolution, the suspension of a Resource Centre when deemed necessary.

Event management is also used to trigger automatic operations such as automatic restart of services in case of detected failures or addition/removal of service instances to a cluster of services to cope with load or to remove faulty instances.

5.3 Incident management

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Incident management is the process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT Service to customers as quickly as possible.

Problem management works together with incident management and change management to ensure that IT service Availability and quality are increased.

The incident record contains the details of an incident. Each incident record documents the lifecycle of a single incident. In EGI records are managed through GGUS[13] - the EGI incident management tool, which is a point of contact for users and service operators.

Failure detection in the monitoring systems and the operations dashboard usually triggers the creation of an incident record through a GGUS ticket. Analysis typically involves different support teams depending on the criticality of the problem: 1st level support, 2nd level support and 3rd level support (offered by the technology providers). If analysis reveals a malfunction in the deployed software, typically 3rd level support opens a problem record in an internal tracking system (GGUS incident records include references to the corresponding problem records if applicable). A problem record that reached 3rd level escalation can trigger a Request For Change (RFCs). RFCs can however be submitted also through GGUS regardless form the detection of incidents and problems.

In EGI different incident escalation procedures exist involving different groups with the appropriate expertise, depending on the nature of the incident. Operational incidents affecting deployed services follow procedure PROC01 “COD escalation procedure”[14]. On the other hand, security incident follow procedure SEC01 “EGI Security Incident Handling”[15].

Incident response times are reviewed annually.

5.4 Request fulfilment

A service request is defined to be a request from a user for information, or advice, or for a sandard change or for access to an IT service. Service requests are handled by the service desk.

[13] http://helpdesk.egi.eu/
[14] https://wiki.egi.eu/wiki/PROC01
[15] https://documents.egi.eu/document/710

Service desk and *incident management* are handled by the same organization of supporters and are based on the same tool (GGUS) – see Sections 5.2, 5.3 and 5.5.

Service requests can be handled at different levels depending on who administers and operates the relevant service:

- Resource Centre level: requests are typically handled through the local Service Desk.
- Resource infrastructure Provider level: requests are handled through GGUS or locally through a Resource infrastructure Provider-specific Service Desk.
- EGI.eu level: requests are handled through GGUS.

5.5 Problem management

Problem management is the process responsible for managing the lifecycle of all problems, where the problem is defined as the unknown cause of one or more incidents. The primary objectives of problem management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented. The EGI problem management tool is GGUS[16]. The "GGUS ticket" is the *problem record* and it contains the details of the problem (problems are categorized by technical area and the level of criticality) and eventually of its solution. After problem detection, the issuing of a GGUS tickets includes the following activities: problem record being raised, problem logging, problem categorization, and problem prioritization. Problem closure is allowed only after a workaround is identified or a fix has been released. In case of a software issue, the problem record is set to ON HOLD during patched development, and is finally set to IN PROGRESS when the software update is in certification.

The EGI problem management process is mainly of reactive nature, and involves various EGI stakeholders:

- End-users who notify the existence of a problem by issuing a GGUS ticket.
- Operations centre staff on duty and the Resource Centre administrators, who monitor the status of their infrastructure and are notified in case of OPERATIONAL alarms.
- The central Grid Oversight team (COD)[17] who is warned after 5 business days in case of alarms that have not been correctly handled by the related administrators and/or by the local staff of the Operations Centres.

Proactive problem management is initiated in Service Operation, but is generally driven as part of Continual Service Improvement. In EGI the central Grid oversight team is responsible of monitoring the performance results of the EGI Resource Centres and Operations Centres, and of collecting justifications from underperforming service providers. Proactive problem management is based on the analysis of the incident records collected on a monthly basis.

Proactive problem management and proactive problem analysis are supported by the EGI monitoring infrastructure, however given the scale of the infrastructure this activity is complex if conducted at EGI-level. Proactive problem management needs more development as it is currently mainly delegated to Operations Centres and Resource Centres.

Vulnerabilities can be proactively identified when a security problem is identified in the deployed software. In case of CRITICAL vulnerabilities, the EGI Problem Management procedure requires in this case to follow a specific escalation procedure which is called "Critical Vulnerability Operational Procedure"[18].

[16] http://helpdesk.egi.eu/
[17] https://wiki.egi.eu/wiki/Grid_operations_oversight
[18] https://documents.egi.eu/document/283

5.6 Access management

Users are identified through X.509 certificates as members of a Virtual Organization groups. Authorization is based on VO user membership and roles, and is usually managed at a VO-level instead of a per-user level. VO access requests are typically handled through Service Requests to the relevant Service Desk. Enabling of VO-level access to resources across multiple administration domains (VO access management) is currently managed and controlled manually, it requires negotiation and agreement with the Resource Centres, and this can introduce delays after a new VO is created when the requested access is highly distributed.

Gap Analysis: This process requires further development in EGI.

5.7 Functions

5.7.1 Service desk

The EGI service desk – based on GGUS – is the primary point of contact for international Virtual Organizations (VOs) and their member users when there is a service disruption, for service requests or even for some categories of Request for Change. The service desk provides a point of communication to the users and a point of coordination for several IT groups and processes.

5.7.2 Technical management

Technical management provides detailed technical skills and resources needed to support the on-going operation of the IT infrastructure, for example for the 2nd level support. Technical management also plays an important role in:

- Design: requirements about the deployed technologies, scalability, Availability and future directions are periodically gathered and prioritized, and finally negotiated with external Technology Providers.
- Testing: technologies are validated and incrementally deployed for safe change management.
- Capabilities that are part of the Unified Middleware Distributed are released and made available from EGI repositories.

5.7.3 Application management

The application is defined as the software that provides functions that are required by an IT service. Each application may be part of more than one IT service. An application runs on one or more servers or clients. In EGI Grid middleware is the set of applications that is deployed at different levels to allow secure and authenticated access to Grid resources, and user community portals. Grid middleware is deployed: at Resource Centres (Grid middleware for direct access to resources), centrally by Resource infrastructure Providers (workload management services, data transfer services, authentication services, information discovery services etc.), and by EGI.eu (multi-VO services, catch all services, central operational tools, etc.).

The application management function supports and maintains operational applications and also plays an important role in the design, testing and improvement of applications that form part of IT services.

In EGI this function is distributed across different departments:

- The Technology unit is responsible of specifying quality criteria, and of verifying the software.
- The Operations unit is responsible of Grid services administration and staged rollout of new versions.

5.7.4 IT operations management

IT operations management is the function responsible for the daily operational activities needed to manage the IT infrastructure. This is done according to the performance targets and service hours defined in Operational Level Agreements. Operations management is distributed across multiple organizations:

- Resource Centres for the services that are operated within their administration domain;
- Resource infrastructure Providers for the local Grid services;
- EGI.eu for the operation of central services and the oversight of the distributed operational activities carried out by Resource Centres and Resource infrastructure Providers. EGI.eu central services are usually outsourced to a number of partners.

IT Operations Management is supported by various types of documentation: procedures, manuals, FAQs, how-TOs, troubleshooting guides and best practices [DOC].

6 CONTINUAL SERVICE IMPROVEMENT

Continual service Improvement is responsible for managing improvements to IT service management processes and IT services. The performance of the IT service provider is continually measured and improvements are made to processes, IT services and IT infrastructure in order to increase efficiency, effectiveness and cost effectiveness [IT-C].

6.1 Improvement process

The improvement process comprises seven different steps.

1. **Definition of services to monitor**. All the Grid services that are part of the operations service asset identified in section 2.1 have to be monitored to ensure the smooth running and the adherence to the service targets defined for the Service Level Management.
2. **Definition of what can be monitored**. The SAM framework currently monitors Grid services that are operated at the Resource Centre, Resource infrastructure Provider and at EGI Global (EGI.eu) level. Currently, the monitoring framework is being expanded to include more tests, especially for the EGI Global tools. However, the Availability and Reliability reporting system is limited to Grid services operated by the Resource Centres and to a subset of those provided by Resource infrastructure Providers. Support services are also monitored by collecting statistics per Support Unit and Operations Centre about various metrics, such as response time to an incident record, time to resolve the incident and assignment time from first level support to second level. Monitoring of support services offered by the Resource Centres is not centrally managed and it is delegated to the Operations Centres. Monitoring of operations services is automated through the operations dashboard to ensure that incident records are properly handled both by Resource Centres and Operations Centres. Escalation mechanisms are available to report centrally about incidents that are not being timely addressed. Finally, EGI.eu and NGI coordination services are assessed annually and results are made publicly available[19].
3. **Processing the data**. Monitoring of Grid Services and Infrastructure and Tool services is managed in a real time reactive way. Resource Centre and Resource infrastructure Provider Grid services Availability/Reliability statistics are reported upon on a monthly basis. Coordination Services are assessed annually.
4. **Analysis of the data**. Grid Services and Infrastructure and Tool services monitoring results are analysed in a real-time fashion. Resource Centre and Resource infrastructure Provider performance are evaluated as part of the EGI oversight activities on a monthly basis. Coordination performance is analysed by the EGI Policy Boards.
5. **Presenting and using this data**. Monitoring and performance data are publicly available through various means: the SAM portal[20] and the EGI operations wiki [PERF].
6. **Implement corrective actions**. In case of incidents detected by the monitoring tools a incident record is registered in GGUS by the operators. On the other hand, Resource Centres that under-perform are requested to provide justifications through GGUS ticket, or in case of prolonged issues for three consecutive calendar months the Resource Centres are suspended. In case of underperforming Resource infrastructure Providers, these are requested to present to EGI.eu a proposal for service enhancement. Finally, for issues that concern coordination tasks, the EGI-InSPIRE Project Management Board and the EGI.eu Executive Board are the policy boards responsible of deciding the most suitable corrective action.

[19] https://wiki.egi.eu/wiki/EGI-inSPIRE_SA1#Assessment_of_Operational_Services
[20] https://Grid-monitoring.cern.ch/myegi/

7 CONCLUSIONS AND FUTURE WORK

The deliverable identifies four operations Services Units and the related providers and users. The analysis conducted for each of the ITIL stages indicates that several processes need to be implemented or expanded. In what follows the main area of work are identified.

In the service strategy stage service costs of the four service categories need to be estimated. This equally applies to Global Services and Local Services. Estimation of costs is necessary to proceed with an analysis of sustainability, to analyse the need for a reduction of operational costs and to define the operations services business model. In addition to this, processes are missing for an integrated demand management across the various resource capacity providers in EGI.

In the service design stage, supplier management and capacity management are currently missing. Supplier management will be developed with the consolidation of the EGI business model. As EGI is a large scale distributed infrastructure that spans multiple service administration domains and service providers, both coordinated capacity management and planning need to be extended. These processes currently exist at a Resource Centre level but are missing at a global level. This process is extremely important for the support of user communities that do not contribute own resources to the infrastructure. A related problem affecting the service operations stage is the lack of global-level access management. Currently, Virtual Organizations that have been registered and approved at an EGI level need to be granted access in the various administration domains. This is currently a fragmented and slow process that introduces delays in the enabling of a new community.

Service transition is currently a well-developed stage that is based on the coordinated collaboration of two EGI-InSPIRE activities (SA1 and SA2). However, because of the multiple service administration domains involved, various existing processes could be considered for an extension. Firstly, a global-level configuration management system and process are missing. GOCDB only provides a very limited set of configuration management system features, and just limited to Grid software assets. Thus, the need for a further development needs to be evaluated. Secondly, process documentation may require extension (as opposed to activity documentation applicable to individual service instances, which is already well covered in EGI operational procedures). Other processes to be evaluated for more development are: knowledge management and transition planning and support.

Because of the highly distributed nature of the teams involved in the operations of the infrastructure and the large amount of knowledge available in various forms, management of the existing knowledge base is currently not uniformly structured, and in particular it is not tightly coordinated among different EGI service areas. Examples of activities that need to be strengthened are: status assessment, lifecycle management, assessment of impact of existing document, analysis of demand.

Proactive problem management and proactive problem analysis are supported by the EGI monitoring infrastructure, however given the scale of the infrastructure this activity is complex if conducted at EGI-level. Proactive problem management needs more development as it is currently mainly delegated to Operations Centres and Resource Centres.

Finally, transition planning and support is a process usually applicable to Resource Centre and Resource infrastructure Provider services that are deployed at large scale, whilst transition of EGI.eu Global Services is not subject to structured planning. It is necessary to extend it to this service category in order to ensure quality of service during transition.

The ITIL conformance study conducted in this deliverable will support future strategy planning activities that concern the analysis of costs, of sustainability and of the business model applicable to the EGI operational services. In addition, the ITIL conformance of operational processes will be periodically reviewed.

8 REFERENCES

ADB	EGI Application Database (http://appdb.egi.eu/)
ACE	Kalmady, R.; Chand, P.; Vaibhav, K. et alt.; Computation of Service Availability Metrics in ACE (https://tomtools.cern.ch/confluence/download/attachments/2261694/Ace_Service_Availability_Computation.pdf?version=1&modificationDate=1314361543000), Aug 2011
ARC	EGI Operations Architecture, EGI-InSPIRE Deliverable D4.1, Jan 2011 (https://documents.egi.eu/document/218)
DOC	EGI Operations Documentation (https://wiki.egi.eu/wiki/Documentation)
EMI	European Middleware Initiative (http://www.eu-emi.eu/)
GOC	EGI Repository of Resource Topology and Information (https://goc.egi.eu/)
IGALC	Iniciativa de Grid de America Latina (http://www.igalc.org/)
IT-C	Continual Service Improvement, Information Technology Infrastructure Library, Office of Government Commerce, Publisher: TSO, 2011
IT-D	Service Design, Information Technology Infrastructure Library, Office of Government Commerce, Publisher: TSO, 2011
IT-O	Service Operation, Information Technology Infrastructure Library, Office of Government Commerce, Publisher: TSO, 2011
IT-S	Service Strategy, Information Technology Infrastructure Library, Office of Government Commerce, Publisher: TSO, 2011
IT-T	Service Transition, Information Technology Infrastructure Library, Office of Government Commerce, Publisher: TSO, 2011
MON	Infrastructure Area Work Plan and Status Report, European Middleware Initiative Deliverable DJRA1.4.2, June 2011 (https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDJRA142)
MOU	EGI Resource Infrastructure Provider MoU Template (https://documents.egi.eu/document/215)
MS208	EGI Membership of the EUGridPMA, EGI-InSPIRE Milestone MS208 (https://documents.egi.eu/document/38)
MS209	Security Policies within EGI, EGI-InSPIRE Milestone MS209, July 2011 (https://documents.egi.eu/document/210)
MS409	Deploying software into the EGI Production Infrastructure, EGI-InSPIRE Milestone MS409, July 2011 (https://documents.egi.eu/document/478)
NEWS	Operations News Feed (http://operations-portal.egi.eu/?limit=40)
OMB	Operations Management Board Terms of Reference (https://documents.egi.eu/document/117)
OTAG	Operational Tools Advisory Group Terms of Reference

	(https://documents.egi.eu/document/103)
PERF	EGI Availability and Reliability Monthly Statistics (https://wiki.egi.eu/wiki/Availability_and_Reliability_monthly_statistics)
POL	EGI Policies and Procedures (https://wiki.egi.eu/wiki/PDT:Policies_and_Procedures)
PRE	EGI Operations in the press (https://wiki.egi.eu/wiki/EGI_Operations_in_the_press)
PROC	Operations Procedures (https://wiki.egi.eu/wiki/Operations_Procedures)
PROC09	Resource Centre Registration and Certification Procedure, EGI Procedure PROC09 (https://wiki.egi.eu/wiki/PROC09)
PROC10	Procedure for the Recomputation of SAM Results and Availability/Reliability (https://wiki.egi.eu/wiki/PROC10)
RCOLA	Resource Centre Operational Level Agreement, May 2011 (https://documents.egi.eu/document/31)
RPOLA	Resource infrastructure Provider Operational Level Agreement (https://documents.egi.eu/document/463)
REQ	EGI Operations Requirements (https://wiki.egi.eu/wiki/Middleware#Existing_requirements)
ROD	Regional Operator on Duty Newsletters (https://documents.egi.eu/secure/ShowDocument?docid=298)
SAG	South African Grid Initiative (http://www.saGrid.ac.za/)
SEC	EGI Security Procedures (https://wiki.egi.eu/wiki/Operational_Procedures#Security)
SEC03	Critical Vulnerability Operational Procedure (https://documents.egi.eu/document/283)
SOR	EGI Operations Statement of Requirements (https://wiki.egi.eu/wiki/Middleware#OMB_Statement_of_Requirements)
SRT	Staged Rollout Template for Early Adopters (https://documents.egi.eu/document/254)
SRW	Staged Rollout Procedures (https://wiki.egi.eu/wiki/Staged-rollout-procedures)
TCB	Technology Coordination Board Terms of Referene (https://documents.egi.eu/document/109)
TMP	EGI Training Market Place (http://www.egi.eu/user-support/training_marketplace/)