1.5   Service Activities and associated work plan

1.5.1   Overall Strategy

The service activities in EGI-InSPIRE are aimed at ensuring that the Grid infrastructure supports the different Science communities in a way that is both efficient and sustainable. This aim will be achieved by:

- operating the production Grid infrastructure (SA1),
- providing a software infrastructure through the coordination of external software providers, appropriate middleware component repositories, support tools and procedures, and a support unit for investigating software issues found in production (SA2),
- providing specific higher-level services for the needs of the communities that are presently heavy users of the Grid (SA3).

The main actors for SA1 activities will be the NGIs, coordinated by EGI.eu, and the infrastructure will be truly pan-European, building on the Grid established by the EGEE projects, but covering also the geographical areas served by Baltic-Grid and SEE-Grid, as well as many East-European countries and Israel. Full interoperability will be pursued within this large European area and increasing interoperation will continue to be ensured with USA, Canada, Latin America, China, Taiwan, and Japan.

The SA2 activity will establish formal agreements with external software providers to supply software components that will form the basis of the UMD release. It is expected that the majority of these components will be sourced initially from the proposed EMI project.

The heavy user communities will both continue to use and contribute to the evolution of the production infrastructure, which they have been doing as early adopters for many years. The SA3 services will complement the ones deployed as general EGI infrastructure and be candidates to become part of the general infrastructure.

Together these three service activities will provide a production infrastructure bringing distributed computing and storage resources together through high performance networking to support researchers in the European Research Area. The SA2 activity will capture the requirements coming from the resource providers and the user communities and ensure these are met through the external technology providers. These technologies will be deployed and integrated across Europe to provide the infrastructure necessary to support world-class research. Through the engagement of the heavy user communities and the resource providers coherent and rapid feedback can be provided to the technology providers to drive their innovation to better meet the needs of the research community.

1.5.2   Relationship between Service Activities

Table 9: Work Package List for EGI-InSPIRE Service Activities

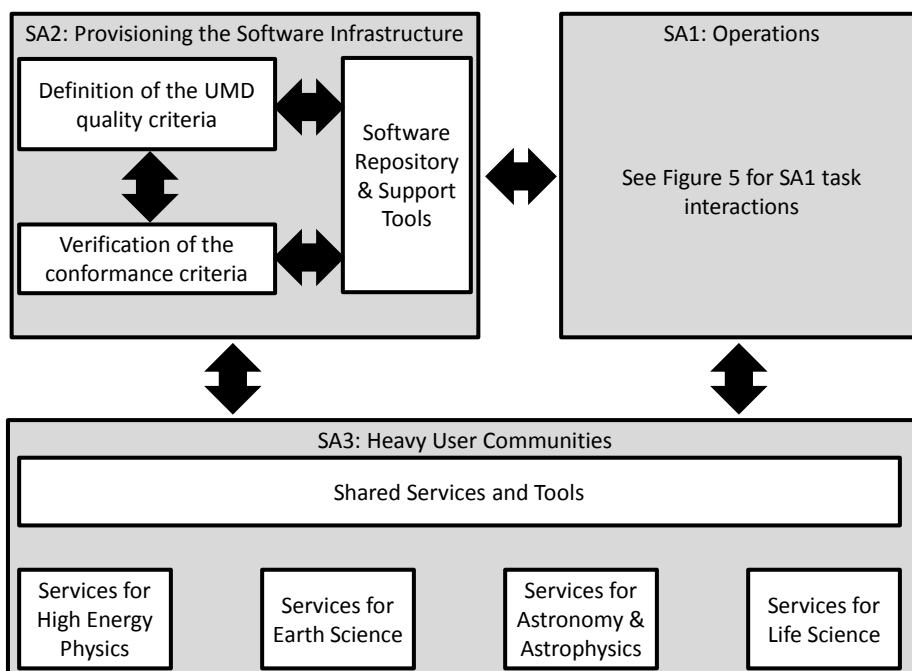| Work package No	Work package title	Type of activity	Lead partic no.	Lead partic. short name	Person-months	Start month	End month
SA1	Operations	SVC	1	EGI.eu	5081	1	48
SA2	Provisioning the Software Infrastructure	SVC	1	EGI.eu	487	1	48
SA3	Services for the Heavy User Communities	SVC	35	CERN	727	1	36
	TOTAL				6295		

Figure 9: Interaction between the service activities

Table 10: Summary of partner effort for the Support Activities

Partner No.	Short Name	SA1	SA2	SA3	TOTAL
1	EGI.eu	36	36	0	72
2	UPT	28	0	0	28
3	IIAP NAS RA	19	0	0	19
4	UNI-LINZ	36	0	0	36
5	IPP-BAS	127	0	0	127
6	UIIP NASB	22	0	0	22
7	SWITCH	81	0	0	81
8	UCY	48	0	0	48
9	CESNET	107	95	0	202
10	KIT	350	24	27	401
11	UOBL ETF	71	0	0	71
12	CSIC	415	71	45	531
13	CSC	87	0	18	105
14	CNRS	326	0	83	409
15	GRENA	19	0	0	19
16	GRNET	249	95	0	344
17	SRCE	83	0	0	83
18	KFKI	107	0	0	107
19	TCD	84	0	18	102
20	IUCC	26	0	0	26
21	INFN	424	47	116	587
22	VU	23	0	0	23
23	RENAM	17	0	0	17
24	UoM	71	0	0	71
25	UKIM	71	0	0	71
26	NCF	198	0	0	198
27	SIGMA	83	0	0	83
28	CYFRONET	177	0	6	177
29	LIP	103	71	0	174
30	IPB	115	0	0	115
31	ARNES	95	0	3	198
32	UI SAV	92	0	18	110
33	TUBITAK ULAKBIM	127	0	0	127
34	STFC	336	0	0	336
35	CERN	59	0	341	400
36	UCPH	81	24	0	105
37	EMBL	0	0	45	45
38	VR-SNIC	99	24	0	123
39	IMCS UL	45	0	0	45
40	e-ARENA	71	0	0	71
41	AGSC	500	0	0	500
	TOTALS	**5081**	**487**	**727**	**6295**

Table 11: Gantt chart for the Service Activities

Activity/Task	Description	1	2	3	4	5	6	7	8	9	10	11	12
SA1	Operations												
TSA1.1	Activity Management	MSA1.1.1					DSA1.1.1					DSA1.2.1	
TSA1.2	A Secure Infrastructure			MSA1.7.1								DSA1.2.1	
TSA1.3	Service Deployment Validation		MSA1.4.1	MSA1.6.1								DSA1.2.1	
TSA1.4	Infrastructure for Grid Management	MSA1.2		MSA1.5.1			DSA1.1.1					DSA1.2.1	
TSA1.5	Accounting											DSA1.2.1	
TSA1.6	Helpdesk Infrastructure		MSA1.3.1									DSA1.2.1	
TSA1.7	Support Teams						MSA1.8.1					DSA1.2.1	
TSA1.8	Providing a Reliable Grid	MSA1.1.1					MSA1.8.1					DSA1.2.1	
SA2	Provisioning the Software Infrastructure												
TSA2.1	Activity Management		MSA2.3.1	DSA2.1.1						DSA2.1.2		DSA2.2.1	
TSA2.2	Definition of the UMD quality criteria			DSA2.1.1						DSA2.1.2		DSA2.2.1	
TSA2.3	Verification of conformance criteria	MSA2.2.1	MSA2.3.1									DSA2.2.1	
TSA2.4	Provision of a software repository and support tools	MSA2.1	MSA2.5.1									DSA2.2.1	
TSA2.5	Deployed Middleware Support Unit		MSA2.4.1									DSA2.2.1	
SA3	Services for Heavy User Communities												
TSA3.1	Activity Management	DSA3.1.1		MSA3.5.1						DSA3.2.1 MSA3.5.2		DSA3.3.1	
TSA3.2	Shared services and tools	DSA3.1.1	MSA3.1.1	MSA3.5.1			MSA3.2.1			DSA3.2.1 MSA3.5.2		DSA3.3.1	
TSA3.3	Services for High Energy Physics (HEP)	DSA3.1.1	MSA3.1.1	MSA3.5.1						DSA3.2.1 MSA3.5.2		DSA3.3.1	
TSA3.4	Services for Life Sciences (LS)	DSA3.1.1	MSA3.1.1	MSA3.5.1						DSA3.2.1 MSA3.5.2		DSA3.3.1	MSA3.4.2
TSA3.5	Services for Astronomy and Astrophysics (A&A)	DSA3.1.1	MSA3.1.1	MSA3.5.1						DSA3.2.1 MSA3.5.2		DSA3.3.1	
TSA3.6	Services for Earth Sciences (ES)	DSA3.1.1	MSA3.1.1	MSA3.5.1						DSA3.2.1 MSA3.5.2		DSA3.3.1	

Activity/Task	Description	Project Month showing Deliverables and Milestones											
		13	14	15	16	17	18	19	20	21	22	23	24
SA1	**Operations**												
TSA1.1	Activity Management	MSA1.1.2					DSA1.1.2					DSA1.2.2	
TSA1.2	A Secure Infrastructure			MSA1.7.2								DSA1.2.2	
TSA1.3	Service Deployment Validation		MSA1.4.2	MSA1.6.2								DSA1.2.2	
TSA1.4	Infrastructure for Grid			MSA1.5.2			DSA1.1.2					DSA1.2.2	
TSA1.5	Accounting											DSA1.2.2	
TSA1.6	Helpdesk Infrastructure		MSA1.3.2									DSA1.2.2	
TSA1.7	Support Teams						MSA1.8.2					DSA1.2.2	
TSA1.8	Providing a Reliable Grid	MSA1.1.2					MSA1.8.2					DSA1.2.2	
SA2	**Provisioning the Software Infrastructure**												
TSA2.1	Activity Management		MSA2.3.2	DSA2.1.13						DSA2.1.4		DSA2.2.2	
TSA2.2	Definition of the UMD quality criteria			DSA2.1.13						DSA2.1.4		DSA2.2.2	
TSA2.3	Verification of conformance criteria	MSA2.2.2	MSA2.3.2									DSA2.2.2	
TSA2.4	Provision of a software repository and support tools	MSA2.5.2										DSA2.2.2	
TSA2.5	Deployed Middleware Support Unit		MSA2.4.2									DSA2.2.2	
SA3	**Services for Heavy User Communities**												
TSA3.1	Activity Management	DSA3.1.2		MSA3.5.3						DSA3.2.2 MSA3.5.4		DSA3.3.2	
TSA3.2	Shared services and tools	DSA3.1.2	MSA3.1.2	MSA3.5.3			MSA3.2.2			DSA3.2.2 MSA3.5.4		DSA3.3.2	
TSA3.3	Services for High Energy Physics (HEP)	DSA3.1.2	MSA3.1.2	MSA3.5.3						DSA3.2.2 MSA3.5.4		DSA3.3.2	
TSA3.4	Services for Life Sciences (LS)	DSA3.1.2	MSA3.1.2	MSA3.5.3						DSA3.2.2 MSA3.5.4		DSA3.3.2	MSA3.4.2
TSA3.5	Services for Astronomy and Astrophysics (A&A)	DSA3.1.2	MSA3.1.2	MSA3.5.3						DSA3.2.2 MSA3.5.4		DSA3.3.2	
TSA3.6	Services for Earth Sciences (ES)	DSA3.1.2	MSA3.1.2	MSA3.5.3						DSA3.2.2 MSA3.5.4		DSA3.3.2	

Activity/Task	Description	Project Month showing Deliverables and Milestones											
		25	26	27	28	29	30	31	32	33	34	35	36
SA1	**Operations**												
TSA1.1	Activity Management	MSA1.1.3					DSA1.1.3					DSA1.2.3	
TSA1.2	A Secure Infrastructure			MSA1.7.3								DSA1.2.3	
TSA1.3	Service Deployment Validation		MSA1.4.3	MSA1.6.3			DSA1.4					DSA1.2.3	
TSA1.4	Infrastructure for Grid			MSA1.5.3			DSA1.1.3					DSA1.2.3	
TSA1.5	Accounting											DSA1.2.3	
TSA1.6	Helpdesk Infrastructure		MSA1.3.3									DSA1.2.3	
TSA1.7	Support Teams						MSA1.8.3					DSA1.2.3	
TSA1.8	Providing a Reliable Grid	MSA1.1.3					MSA1.8.3					DSA1.2.3	
SA2	**Provisioning the Software Infrastructure**												
TSA2.1	Activity Management		MSA2.3.3	DSA2.1.5						DSA2.1.6		DSA2.2.3	
TSA2.2	Definition of the UMD			DSA2.1.5						DSA2.1.6		DSA2.2.3	
TSA2.3	Verification of conformance criteria	MSA2.2.3	MSA2.3.3									DSA2.2.3	
TSA2.4	Provision of a software repository and support tools	MSA2.5.3										DSA2.2.3	
TSA2.5	Support Unit for		MSA2.4.3									DSA2.2.3	
SA3	**Services for Heavy User Communities**												
TSA3.1	Activity Management	DSA3.1.3		MSA3.5.5						DSA3.2.3 MSA3.5.6		DSA3.3.3	
TSA3.2	Shared services and tools	DSA3.1.3	MSA3.1.3	MSA3.5.5			MSA3.2.3			DSA3.2.3 MSA3.5.6		DSA3.3.3	
TSA3.3	Services for High Energy Physics (HEP)	DSA3.1.3	MSA3.1.3	MSA3.5.5						DSA3.2.3 MSA3.5.6		DSA3.3.3	
TSA3.4	Services for Life Sciences (LS)	DSA3.1.3	MSA3.1.3	MSA3.5.5						DSA3.2.3 MSA3.5.6		DSA3.3.3	MSA3.4.3
TSA3.5	Services for Astronomy and Astrophysics (A&A)	DSA3.1.3	MSA3.1.3	MSA3.5.5						DSA3.2.3 MSA3.5.6		DSA3.3.3	
TSA3.6	Services for Earth Sciences (ES)	DSA3.1.3	MSA3.1.3	MSA3.5.5						DSA3.2.3 MSA3.5.6		DSA3.3.3	

Activity/Task	Description	Project Month showing Deliverables and Milestones											
		37	38	39	40	41	42	43	44	45	46	47	48
SA1	**Operations**												
TSA1.1	Activity Management	MSA1.1.4					DSA1.1.4					DSA1.2.4	
TSA1.2	A Secure Infrastructure			MSA1.7.4								DSA1.2.4	
TSA1.3	Service Deployment Validation		MSA1.4.4	MSA1.6.4								DSA1.2.4	
TSA1.4	Infrastructure for Grid Management						DSA1.1.4					DSA1.2.4	
TSA1.5	Accounting											DSA1.2.4	
TSA1.6	Helpdesk Infrastructure		MSA1.3.4									DSA1.2.4	
TSA1.7	Support Teams						MSA1.8.4					DSA1.2.4	
TSA1.8	Providing a Reliable Grid	MSA1.1.4					MSA1.8.4					DSA1.2.4	
SA2	**Provisioning the Software Infrastructure**												
TSA2.1	Activity Management		MSA2.3.4	DSA2.1.7						DSA2.1.8		DSA2.2.4	
TSA2.2	Definition of the UMD quality criteria			DSA2.1.7						DSA2.1.8		DSA2.2.4	
TSA2.3	Verification of conformance criteria	MSA2.2.4	MSA2.3.4									DSA2.2.4	
TSA2.4	Provision of a software repository and support tools	MSA2.5.4										DSA2.2.4	
TSA2.5	Deployed Middleware Support Unit		MSA2.4.4									DSA2.2.4	
SA3	**Services for Heavy User Communities**												
TSA3.1	Activity Management												
TSA3.2	Shared services and tools												
TSA3.3	Services for High Energy Physics (HEP)												
TSA3.4	Services for Life Sciences (LS)												
TSA3.5	Services for Astronomy and Astrophysics (A&A)												
TSA3.6	Services for Earth Sciences (ES)												

1.5.3   Work Package SA1: Operations

1.5.3.1 Summary

Work package number	SA1		**Start date or starting event:**		1/5/2010	
Work package title	Operations					
Activity type	SVC					
Participant number	1	2	3	4	5	6	7
Participant short name	EGI.eu	UPT	IIAP NAS RA	UNI LINZ	IPP-BAS	UIIP NASB	SWITCH
Person-months per participant	36	28	19	36	127	22	81
Participant number	8	9	10	11	12	13	14
Participant short name	UCY	CESNET	KIT	UOBL ETF	CSIC	CSC	CNRS
Person-months per participant	48	107	350	71	415	87	326
Participant number	15	16	17	18	19	20	21
Participant short name	GRENA	GRNET	SRCE	KFKI	TCD	IUCC	INFN
Person-months per participant	19	249	83	107	84	26	424
Participant number	22	23	24	25	26	27	28
Participant short name	VU	RENAM	UoM	UKIM	NCF	SIGMA	CYFRO NET
Person-months per participant	23	17	71	71	198	83	177
Participant number	29	30	31	32	33	34	35
Participant short name	LIP	IPB	ARNES	IISAS	TUBITAK ULAKBIM	STFC	CERN
Person-months per participant	103	115	95	92	127	336	59
Participant number	36	38	39	40	41		
Participant short name	UCPH	VR-SNIC	IMCS UL	e-ARENA	AGSC	TOTAL	
Person-months per participant	53	99	45	71	500	5081	

Objectives

This activity will coordinate a secure, reliable European-wide production grid infrastructure federated from national grid initiatives that is integrated and interoperates with other grids worldwide. It will:

- Maintain a secure infrastructure through the establishment of the necessary operational security teams
- Validate new releases of the middleware and operational tools through a coordinated staged roll-out to sites
- Establish the monitoring services needed to manage the production grid infrastructure
- Provide a central accounting database and portal where aggregated use of the infrastructure is recorded
- Provide the EGI Helpdesk infrastructure, integrated with national instances, to coordinate activity between the different support teams.

- Establish the necessary support teams within the infrastructure that once integrated with the EGI Helpdesk will respond to user and site support issues
- Provide a reliable and consistent production grid infrastructure through the establishment and monitoring of SLAs, documentation and the provision of core grid services.

Description of work

TSA1.1: Activity Management

The overall management of the activity is led by the Chief Operations Officer, reporting to the Project Director, who coordinates the work of the NGI/EIRO Operations Centres. The Operations Coordination Centre (OCC) consists of the COO and the SA1 Task coordinators. They manage the effective delivery of the (i) the EGI.eu Global Tasks (either running services or coordinating the work of the NGIs and related activities), and (ii) the International Tasks carried out by the NGIs in order to provide an integrated European e-Infrastructure to support the international VOs.

Requested Effort: 36PMs EGI.eu

TSA1.2: A Secure Infrastructure

The aim of this task is to address the various operational security-related risks and to maintain the availability of EGI services. This task covers all aspects of operational security including Security Incident Coordination and Security Vulnerability Handling. It relies on the GOCDB Security contact information and the security related policy work done under NA2.

Requested Effort: 4PMs UPT, 12PMs UNI LINZ, 16PMs IPP-BAS, 16PMs SWITCH, 12PMs CESNET, 20PMs KIT, 4PMs UCPH, 16PMs CSIC, 3PMs CSC, 44PMs CNRS, 4PMs GRNET, 8PMs KFKI, 8PMs TCD, 4PMs IUCC, 12PMs INFN, 4PMs UoM, 4PMs UKIM, 28PMs NCF, 8PMs SIGMA, 12PMs CYFRONET, 8PMs LIP, 8PMs IPB, 12PMs e-ARENA, 8PMs VR SNIC, 4PMs ARNES, 8PMs UI SAV, 8PMs TUBUTAK ULAKBIM, 40PMs STFC

TSA1.3: Service Deployment Validation

This task will ensure that new software releases (for operational tools, and global and site services) will be deployed safely and reliably without any degradation of service to the production grid infrastructure, and while maintaining interoperability with other grids infrastructures. This will be achieved through a managed staged roll-out of middleware and operational tools. In collaboration with NGIs and end-user communities new software releases will be deployed to build operational and user experience.

Requested Effort: 4PMs UPT, 4PMs IIP NAS, 24PMs IPP-BAS, 4PMs SWITCH, 4PMs UCY, 28PMs KIT, 12PMs UCPH, 76PMs CSIC, 8PMs CSC, 32PMs CNRS, 4PMs GRENA, 24PMs GRNET, 4PMs SRCE, 16PMs TCD, 4PMs IUCC, 12PMs INFN, 4PMs IMUL, 4PMs RENAM, 8PMs UoM, 4PMs UKIM, 16PMs NCF, 12PMs CYFRONET, 20PMs LIP, 8PMs IPB, 8PMs e-ARENA, 36PMs VR-SNIC, 20PMs ARNES, 8PMs UI SAV, 12PMs TUBITAK ULAKBIM, 48PMs STFC, 8PMs UBOL ETF

TSA1.4: Infrastructure for Grid Management

The purpose of this task is the deployment of the infrastructure for Grid management consisting of a set of services and tools needed by the NGI/EIRO Operations Centres for the running of the Grid software services, for Grid monitoring (including SLA and security monitoring), and ongoing Grid management. At the core of this infrastructure is a set of monitoring tools to be deployed in all NGIs to monitor their sites. Above this will sit higher-level monitoring of global services and automated measurement of various service and site-reliability metrics.

Requested Effort: 8PMs UPT, 4PMs IIAP NAS, 12PMs UNI LINZ, 36PMs IPP-BAS, 12PMs UIIP NASE, 16PMs SWITCH, 4PMs UCY, 36PMs CESNET, 68PMs KIT, 28PMs UCPH, 72PMs CSIC, 16PMs CSC, 80PMs CNRS, 4PMs GRENA, 60PMs GRNET, 36PMs SRCE, 36PMs KFKI, 24PMs TCD, 8PMs IUCC, 72PMs INFN, 8PMs VU, 12PMs IMCS UL, 4PM RENAM, 20PMs UoM, 16PMs UKIM, 12PMs NCF, 28PMs SIGMA, 56PMs CYFRONET, 12PMs LIP, 8PMs IPB, 32PMs e-ARENA, 16PMs VR-SNIC, 20PMs ARNES, 20PMs UI SAV, 20PMs TUBITAK ULAKBIM, 56PMs STFC, 60PMs CERN, 24PMs UOBL ETF

TSA1.5: Accounting

This task will provide a reliable record of the usage of the infrastructure for users, VOs, NGI and EGI management. Access to data will be restricted according to agreed policies and NGI/EIRO privacy laws. This

task will provide: securely and reliably run accounting repositories for EGI, and if desired at the NGI-level; a portal to provide on-demand visualisation and/or data download. Developments needed to account for additional resources to support new business models are described in JRA1.

Requested Effort: 4PMs UPT, 4PMs IIAP NAS, 8PMs SWITCH, 12PMs CESNET, 12PMs KIT, 4PMs UCPH, 56PMs CSIC, 4PMs CSC, 8PMs CNRS, 4PMs GRENA, 12PMs GRNET, 4PMs SRCE, 4PMs TCD, 4PMs IUCC, 60PMs INFN, 8PMs VU, 4PMs IMCS UL, 4PMs UoM, 4PMs UKIM, 4PMs NCF, 8PMs SIGMA, 8PMs CYFRONET, 8PMs LIP, 4PMs IPB, 4PMs e-ARENA, 8PMs ARNES, 12PMs UI SAV, 8PMs TUBITAK ULAKBIM, 12PMs STFC, 4PMs UOBL ETF

TSA1.6: Helpdesk Infrastructure

This task will provide a central EGI Helpdesk available to all NGIs and related support projects. NGIs will integrate their own national helpdesk into EGIs through an agreed interface or use the EGI Helpdesk remotely. Standard procedures for handling tickets, passing them between helpdesks, escalating them will be established based on the experiences from previous projects.

Requested Effort: 4PMs IIP NAS, 4PMs UNI LINZ, 4PMs SWITCH, 4PMs UCY, 12PMs CESNET, 68PMs KIT, 4PMs UCPH, 56PMs CSIC, 4PMs CSC, 8PMs CNRS, 4PMs GRENA, 12PMs GRNET, 4PMs SRCE, 12PMs KFKI, 4PMs TCD, 28PMs INFN, 4PMs VU, 8PMs UoM, 8PMs UKIM, 4PMs NCF, 8PMs SIGMA, 12PMs CYFRONET, 12PMs LIP, 20PMs IPB, 12PMs VR-SNIC, 8PMs ARNES, 8PMs TUBITAK ULAKBIM, 24PMs STFC, 8PMs UOBL ETF

TSA1.7: Support Teams

This task will bring together the various teams of people handling support issues for users, sites and the network within the production infrastructure. It will not merge them into a common team as the skills required differ, but it will make sure the infrastructure is in place and the teams are trained and resourced and all the required documentation is in place.

Requested Effort: 8PMs UPT, 4PMs IIAP NAS, 12PMs UNI LINZ, 52PMs IPP-BAS, 4PMs UII NASE, 32PMs SWITCH, 12PMs UCY, 36PMs CESNET, 92PMs KIT, 20PMs UCPH, 120PMs CSIC, 16PMs CSC, 96PMs CNRS, 4PMs GRENA, 60PMs GRNET, 12PMs SRCE, 16PMs KFKI, 8PMs TCD, 4PMs IUCC, 196PMs INFN, 8PMs VU, 8PMs IMCS UL, 4PMs RENAM, 20PMs UoM, 20PMs UKIM, 96PMs NCF, 28PMs SIMGA, 48PMs CYFRONET, 28PMs LIP, 48PMs IPB, 16PMs e-ARENA, 16PMs VR-SNIC, 12PMs ARNES, 40PMs UI SAV, 52PMs TUBITAK ULAKBIM, 144PMs STFC, 20PMs UOBL ETF

TSA1.8: Providing a Reliable Grid Infrastructure

This task is to ensure that sites and operational and middleware services are functional, reliable, and responsive. It will achieve this through subtasks on: production grid services, interoperability, best practices and service level agreements. It also has dependencies on other subtasks which manage the human support teams, security, helpdesks, and the monitoring and management infrastructure.

Requested Effort: 4PMs UPT, 4PMs SWITCH, 20PMs UCY, 64PMs KIT,8PMs UCPH, 24PMs CSIC, 32PMs CSC, 64PMs CNRS, 72PMs GRNET, 12PMs SRCE, 36PMs KFKI, 16PMs TCD, 4PMs IUCC, 48PMs INFN, 12PMs IMCS UL, 4PMs RENAM, 8PMs UoM, 16PMs UKIM, 36PMs NCF, 20PMs CYFRONET, 16PMs LIP, 20PMs IPB, 4PMs VR-SNIC, 24PMs ARNES, 8PMs UI SAV, 20PMs TUBITAK ULKBIM, 12PMs STFC

Deliverables (brief description) and month of delivery

Month 6, 18, 30 & 42: DSA1.1.1-4 – EGI Operations Architecture

A technical description of all the operational services needed globally (EGI.eu) and nationally (NGI/EIRO International Tasks). It also defines the operational interfaces that need to be supported by a technology for its integration into the EGI production infrastructure.

Month 11, 23, 35 & 47: DSA1.2.1-4 – Annual Report on the EGI Production Infrastructure

This public report describes the current status and activity that has taken place in the production infrastructure over the last year. It will report on the current status of the NGI & EGI operational structures, the integration of different resources and other production infrastructures within EGI,

Month 18: DSA1.3 – Security Risk Assessment of the EGI Production Infrastructure

A comprehensive review will be undertaken of the current EGI Production Infrastructure to assess its security vulnerabilities and associated risks. This will review will cover the current technologies but also indicate vulnerabilities that will need to be mitigated in new candidate technologies that will be integrated

into the infrastructure.

Month 30: DSA1.4 – Devolution of operational tools and processes to NGIs within a European production infrastructure

A public report describing the regionalised operational tools (from TJRA1.4) that have been developed and how they have been deployed and used within the production infrastructure.

1.5.3.2 Overview

The EGI operations management is built upon the inherited experience of the series of EGEE projects and has been structured into a number of mutually dependent tasks. The interconnection and dependency between them are illustrated by the diagram in Figure 10 below:
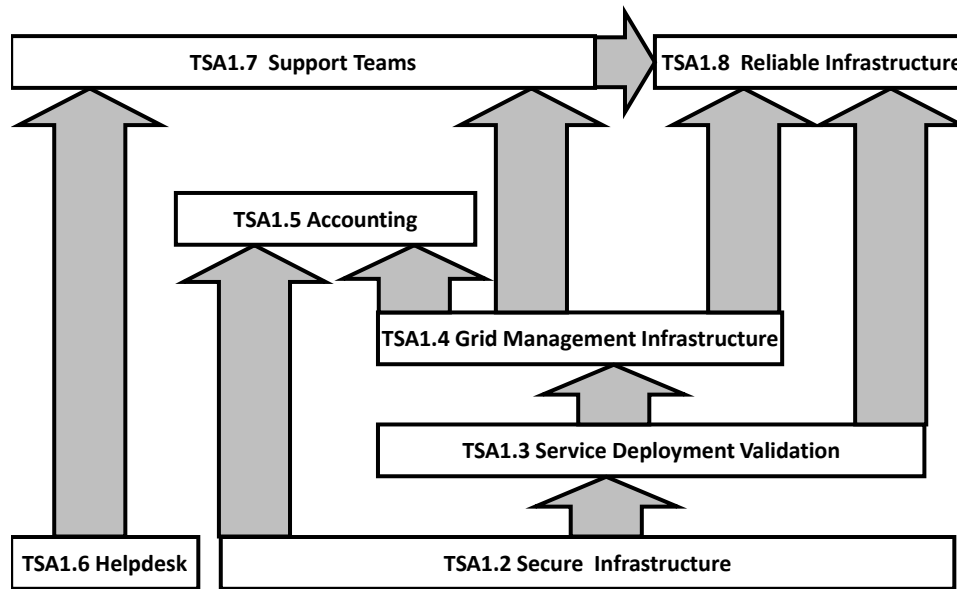
Figure 10: Relationship between SA1 tasks

Two new structures, namely the Operations Management Board (for dealing with policy and management issues – see TNA2.3, Section 1.4.4.4 for details) and the Operations Forum (for dealing with general technical coordination across the activity) and will be established to evolve EGEE's regional operations structure into a set of independent NGIs/EIROs.

The EGI Operations Forum is a technical body led by the COO, where technical issues of general interest concerning all operational activities are discussed, e.g. best practices, procedures, operational interoperability issues, etc. It is an incubator of ideas of new developments, and it provides a means to share experience and know-how between partners. The Operations Forum facilitates the cooperation between the NGIs/EIROs, and between NGIs/EIROs and the SA1 task coordinators. Its activity is structured into two types of groups working under defined charters: working groups and task forces for long-term and short-term technical activities respectively. These technical activities will include stakeholder consultations to review the performance of services and tasks over an extended period and propose changes to requirements, service levels or procedures, etc. Participation is open to all, with representation expected from NGI/EIRO Operations Centre Managers and technical staff; and the operational development teams (see JRA1 for details). Representatives from other infrastructure projects and external software providers will be invited if required.

1.5.3.3 TSA1.1: Activity Management

The SA1 activity is managed by the Chief Operations Officer (COO) who also leads the EGI.eu Operations Team and represents the operational activities within other bodies. The COO leads the SA1 activity and oversees the JRA1 activity (Operational Tool Development) by directing the work of the SA1 Task Coordinators and by working with the NGI/EIRO Operations Centre Managers to achieve the activity's objectives. The COO also organises the EGI Operations Forum.

The COO and the SA1 Task coordinators constitute the Operations Coordination Centre (OCC) that is responsible for the overall management of the activity. The OCC will oversee the execution of the overall SA1 activity, checking the consistency between the different activities, and their relationship with the agreed roadmaps. Policy and future roadmaps will be established through the Operations Management Board (part of NA2).

The COO will also be responsible for defining the operational SLDs between EGI and the NGIs for the NGI International Tasks, and between EGI and NGIs providing the EGI Global Tasks. These SLDs will be monitored and reported through the EGI-InSPIRE Quality Assurance Officer and reviewed periodically.

1.5.3.4 TSA1.2: A Secure Infrastructure

This task covers all aspects of operational security aimed at achieving 'a secure infrastructure' within EGI and relies on site and NGI security contact information maintained in the GOCDB by each NGI. EGI will appoint an 'EGI Security Officer' to coordinate operational security who will be assisted in each NGI by a designated 'NGI Security Officer'. A Software Vulnerability Group will be established to assess threats to the infrastructure arising from software issues.

The EGI Computer Security and Incident Response Team (EGI CSIRT) is an activity aimed at coordinating the operational security activities in the infrastructure, in particular the response to security incidents. As security incidents may affect any resource providers, inside or outside the EGI production infrastructure, the appropriate procedures, information flow and a collaboration based on trust that allows the free exchange of information to protect other infrastructures from an active known threat, has to be implemented to ensure security incidents are dealt with appropriately by the resource providers and the involved CSIRTs. The EGI CSIRT ensures both the coordination with peer grids and with the NGIs and NREN CSIRTs. In addition, the EGI CSIRT acts as a forum to combine efforts and resources from the NGIs in different areas, including Grid security monitoring, Security training and dissemination, and improvements in responses to incidents (e.g. security drills).

Each NGI will appoint an "NGI Security Officer" in order to provide the NGI CSIRT function. A number of NGIs are already implementing this functionality via their local NREN CSIRT. Where this is not the case, a close collaboration with the local NREN CSIRT is highly encouraged. The resulting group of NGI Security Officers collaborate as part of the EGI CSIRT. The EGI CSIRT is led and coordinated by the EGI Security Officer, whose role and mission are defined by security policies approved by EGI and the NGIs.

Alongside this activity, EGI also needs to have the ability to add or remove certificate authorities (as specified by the project and the EGI Council) and will therefore provide its own distribution of the IGTF CA bundle. NGIs may also want to add more CAs, or even remove specific CAs that are incompatible with their national policy. In the latter case, an NGI will need to build its own distribution locally.

The main purpose of the Software Vulnerabilities Group (SVG) is to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents. The SVG will need to interact closely with the operational development teams in JRA1 and the middleware teams through the Software Security Group. SVG will be situated in the Operational Security area in order that it should be recognised as a means of ensuring security of the deployed infrastructure and enforcing the responsible disclosure strategy. As well as handling specific vulnerabilities found, it will actively check that the deployed middleware is secure. Consequently, the SVG will look for strategies for doing this. There is also an educational role for the SVG within the developer community to improve the quality of any newly developed software.

1.5.3.5 TSA1.3: Service Deployment Validation

Processes will be put in place to ensure that new software releases (for both middleware services and operational tools) will be deployed safely and reliably without any degradation of service to the production grid infrastructure.

Coordination by EGI.eu of the software roll-out process, through staged deployment and functional validation for all software, ensures that updates move from certification and into production as quickly as possible, while also assuring that the updates are suitable for deployment throughout the production infrastructure. EGI.eu will provide strategic leadership, for example concerning significant changes to processes, and to ensure that resource sites are encouraged to upgrade whenever new critical software updates are released. This coordination is needed as the

prompt alignment of the services and components to the latest releases contributes to better functionality and availability of the overall infrastructure. The staged rollout of new software releases will include the validation of its correct operation within the NGIs, with user communities, and with collaborating infrastructures worldwide.

1.5.3.6 TSA1.4: Infrastructure for Grid Management

Infrastructure is needed by the NGI/EIRO Operations Centres for the monitoring of the running Grid software services to ensure their correct operation. The running of such services requires a combination of EGI.eu Global Tasks and NGI/EIRO International Tasks. An initial list of services and tools is provided below. More services are expected to be defined and implemented during the project.

Monitoring information is gathered using an infrastructure that includes Nagios, SAM, and other tools (e.g. GridMap, Gridview, ...). This data is stored in repositories, and used to publish site and service status information. During the project, the monitoring infrastructure will move from the regional model (inherited from the EGEE-III project) to a national infrastructure. EGI.eu will gather statistics, maintain the schema for central publication of site and service status information, deploy the central instances of monitoring-related tools such as the dashboard and the alarm system, and prepare the national and VO oriented views of the site performance reports. The NGIs/EIROs will monitor their sites, run their local monitoring infrastructure for their hosted service instances, validate the information and publish the collected information to a central metric store.

A light-weight end-to-end network performance monitoring infrastructure will be coordinated and its configuration support provided by EGI.eu. This will be used to troubleshoot network connectivity issues, such as end-to-end network performance affecting Grid data transfers. The deployment of end-to-end monitoring tools is a responsibility of the Grid site managers, coordinated by their respective NGIs/EIROs.

Many aspects of operations rely on the availability of information (as applicable) from NGIs about service nodes, contact details, security contacts, certification status, sites in scheduled downtime, etc. The GOCDB provides all such information through a central database containing a sub-database per operations region (these will be managed by the regions).

EGI.eu is responsible for the coordination of the tool deployment, and of the running the central service. The NGIs/EIROs are responsible for maintaining data about itself and its sites, for running the NGI service instance (where applicable) and in this case also for publishing the agreed schema to the central database.

The CIC Operations Portals and NGI Dashboard provide different "views" of the data according to the role of the customer (Grid operators, VOs, Grid site managers, Region Operations Managers, etc.). The portal also provides services including the VO registration tool, the broadcast and downtime tool, the periodic operations report submission system, and the regional dashboard. The CIC portal will be maintained centrally with the management distributed to regions and VOs. EGI.eu runs the central portal, automates the gathering of the required information and coordinating the activity, while the NGI is responsible for maintaining the relevant information about their infrastructure and VOs, and to run the service locally as required.

1.5.3.7 TSA1.5: Accounting

Infrastructure usage has to be reliably recorded according to agreed policies and local NGI/EIRO privacy laws in order to plan for its future provisioning. Grid accounting repositories (both central and regional) need to be maintained so that stakeholders such as VO managers and VO members, resource providers, NGI/EIRO Operations Centres, VRCs etc. will obtain an overview of the resource usage across the different domains of the production infrastructure. A deployment plan will be defined for regionalised versions of the accounting repository as required by NGIs. The central repository will remain the default repository for international VOs.

EGI.eu will coordinate this task, run the central service and central repository, maintain the schema of the centrally-held information and be responsible for the monitoring of the publication of usage records from NGIs/EIROs into the central repository instance. The NGIs are responsible for running the local accounting repository, for maintaining and validating data about all usage made of its sites and for publishing data on international VOs to the appropriate repository.

EGI.eu is also responsible for the central accounting portal which allows dynamic queries against aggregated accounting data produced by the NGI/EIROs-level by different accounting sensors (e.g. APEL, DGAS, SGAS,

Gratia) into just one place for an aggregated view and using topology information extracted from the GOCDB. The set of information about usage is selectively displayed depending on the client's role to comply with EGI's privacy policy.

1.5.3.8 TSA1.6: Helpdesk Infrastructure

The EGI Helpdesk is a distributed infrastructure consisting of a central helpdesk interconnected with a collection of local NGI/EIRO Helpdesks. This provides a regional support system with central coordination undertaken by EGI.eu. The evolution of this service is under the responsibility of the User Services Advisory Group (USAG).

The central instance provides access to a ticketing system that allows for the bi-directional exchange of tickets with the remote NGI Helpdesks to ensure that tickets opened centrally are handled by the appropriate support team. For example, those opened locally can be passed to the central instance or other areas, while user and operational problem tickets can be opened centrally and subsequently routed to the NGI local support infrastructures. The number of independent NGI Helpdesks integrated into the central instance will grow over the course of the project as the NGIs mature. Until then NGIs could use the central instance to respond to any assigned tickets. EGI.eu is responsible for the deployment and operation of the central instance and defining and supporting an interface through which local instances can interoperate with the central service. The NGI is responsible for deployment, maintenance of any local instance and its integration through a defined interface into the central instance.

1.5.3.9 TSA1.7: Support Teams

This task supports the Ticket Triage teams within EGI.eu and the teams carrying out the user support work within the NGI. The Ticket Triage team (or Ticket Processing Management – TPM) is responsible for the monitoring and routing of all active tickets in the Grid user support system to the appropriate second-line specialized support units. These support units will be in the operational tasks, in other activities, or other projects like the VRCs. In the NGIs, the teams support their local users of international VOs.

At the core of the Operational Support Teams' work is the monitoring and support of the sites through a ticketing system which will contain issues raised as a result of the monitoring system, VOs, users and system administrators. This ensures that the International VOs get the services agreed through EGI. The practical work includes:
- Monitoring and help desk shifts
- Triage of incoming problems, assignment of tickets to the 2nd line support units, ticket escalation, ticket follow-up, suspension of sites if needed, etc.
- Certification of the sites entering the NGI Grid and thus in the EGI Grid, with the rules agreed with EGI, according to the site category and SLD.
- The interface with the NREN is specifically required for troubleshooting of connectivity problems, test for advancement in technologies etc.
- Maintenance of web pages for FAQ, best practices etc.
- Operation of a ticketing system integrated with the EGI Helpdesk

The bulk of the work is done by NGIs using their own monitoring infrastructure for their own sites and users but there is a central role in coordination so that the international VOs receive the same level of service and cross-border issues are resolved.

Coordination of resource allocation and brokering between VOs and the NGIs is required by VOs and provided by EGI.eu in collaboration with the NGIs. This ensures that suitable resources (compute, storage, deployed services) are allocated to the VO within the production infrastructure, to meet their requirements and the availability of resources. The central Network Support role within EGI.eu maintains the design of the network operations, handles issues affecting international VOs, and allows EGI to keep the state of the network under control, and to establish links between Grid operations and network operations.

1.5.3.10 TSA1.8: Providing A Reliable Grid Infrastructure

This task ensures that sites, operational and middleware services are functional, reliable, and responsive by providing Core Software Services, Interoperability, and the continual refinement of best practice policy and procedures to achieve this.

The Core Software Services are those required by a VO in order to operate, i.e., where there is a single instance in the infrastructure or in a region. Catch-all instances are provided by EGI.eu to support small user communities.

Examples of gLite Core Software Services are: the VO management service (e.g. VOMS), the File catalogue and transfer services (e.g. LFC and FTS), Job management services (e.g. WMS), Information services (e.g. BDII), Security services, etc. EGI.eu coordinates the provision of services to be delivered by an NGI as required by the VOs.

Interoperability and interoperation of the EGI infrastructure with others is coordinated by EGI.eu and covers the availability of common tests for monitoring of site status, the operational tools interfaces (including the interconnection between helpdesks/ticketing systems), the procedures and the operational activities allowing the NGIs to interoperate, the interconnection with other regional grids (e.g. Asia-Pacific regional Grids, OSG, Naregi, and related infrastructure projects). NGIs may work on interoperation with other grids of relevance to them but only with EGI.eu approval. Interoperation of grids within a country is considered an internal national matter.

The definition of best practices, mandatory operations procedures and operational requirements becomes increasingly important as the infrastructure scales out to include more NGIs yet remain a seamless and integrated resource for all. Documenting best practices is an essential step in disseminating knowledge of how an efficient and effective grid infrastructure operates. While obeying this best practice is not mandatory, it will be particularly useful for the nascent NGIs who are new to EGI and will become independent during the project. The operational process during the first year of the project will be mainly based on existing EGEE procedures and practices. These will be redefined to adapt them to the needs of new NGIs joining the infrastructure, and to the new operations architecture that will be defined by the EGI project.

SLDs will be an agreed between NGIs and their sites, there will be overseen centrally so that VOs will be assured of the quality and performance of the sites on which they run. This task will use the outputs of various monitoring tools to evaluate site quality metrics presented through the Metrics Portal (see TJRA1.2.7).

1.5.3.11 Deliverables

Deliverable Number	Deliverable name	Work package(s) involved	Nature	Dissemi -nation level	Delivery date (project month)
DSA1.1.1-4	EGI Operations Architecture	SA1	R	PU	M06, M18, M30, M42
DSA1.2.1-4	Annual Report on the EGI Production Infrastructure	SA1	R	PU	M11, M23, M35, M47
DSA1.3	Security Risk Assessment of the EGI infrastructure.	SA1	R	PU	M18
DSA1.4	Devolution of operational tools and processes to NGIs within a European production infrastructure	SA1	R	PU	M30

1.5.3.12 Milestones

Milestone number	Milestone name	Work package(s) involved	Expected date	Means of verification
MSA1.1.1-4	Service Level Descriptions (SLDs) within the EGI production infrastructure.	SA1	M01, M13, M25, M37	Report defining the SLDs expected from the NGI & EIRO resource providers and any changes needed in the operational tools to support the SLDs.
MSA1.2	Operational Tools regionalisation status	SA1	M01	Report assessing the current status of the regionalisation of the operation tools and prioritising the remaining work that needs to be under taken by TJRA1.3.

MSA1.3.1-4	EGI Helpdesk and the NGI Support Units	SA1	M02, M14, M26, M38	Description of the operational procedures and NGI support units within the production infrastructure including the network support provided in EGI through its service providers.
MSA1.4.1-4	Deploying Software into the EGI production infrastructure	SA1	M02, M14, M25, M38	Description of the procedures used to take new software releases (of middleware or operational tools) from the software repository for staged rollout as a precursor to wide scale deployment in production.
MSA1.5.1-3	Deployment plan for the distribution of operational tools to the NGIs/EIROs	SA1	M03, M15, M27	A plan for the deployment of regionalised variations of the operational tools to the NGIs will be established based on the status of the tools at the end of EGEE-III and after TJRA1.3.
MSA1.6.1-4	Integrating Resources into the EGI Production Infrastructures	SA1	M03, M15, M27, M39	Definition of the operational interfaces an infrastructure and its middleware must support for it to be integrated into the production infrastructure. This informs NGIs deploying software that is not part of the UMD release or infrastructures integrating their resources with EGI as to the steps they must take to be part of the production infrastructure.
MSA1.7.1-4	Operational Security Procedures	SA1	M03, M15, M27, M39	The report defines the security related operational procedures for handling security indents and vulnerabilities.
MSA1.8.1-4	EGI Operational Procedures	SA1	M6, M18, M30, M42	Report covering all operational activities within EGI

1.5.3.13 Risk Assessment and Mitigation

Risks	Impact	Probability of Occurrence	Mitigation
NGIs will deploy their own middleware solutions that will not be interoperable with others.	Non-interoperable middleware stacks will shatter the transparent infrastructure being offered to users. Users will have to customise their client and application for particular sites, rather than for the infrastructure as a whole.	High	The EGI model accepts that NGIs might deploy their own middleware solutions and the interoperation and interoperability task in this activity will validate new releases with the currently deployed infrastructure. The MCB, through the UMD criteria, will define the interfaces that the public-site services must support to provide an interoperable solution. Software that has been shown to meet these criteria will be endorsed by EGI even if it is not distributed as part of the UMD solution.

A security vulnerability could be discovered in software deployed within the production infrastructure.	An exploitable vulnerability could allow a malicious user to use the grid for denial of service attacks on high profile websites that could bring bad press to European DCIs.	High	The infrastructure as a whole, each NGI, and each site in the infrastructure must provide a security officer and backup. These will be used by the EGI Security Officer to communicate and act on security issues for the sites to promptly implement any mandated changes. This protocol will be tested with regular security challenges. The Software Vulnerability Group will proactively assess the impact of reported issues on the infrastructure, and the Software Security Group will work to improve the quality and coherence of security related grid specific code.
Software within UMD is found to fail when used in production.	The functionality offered within EGI stagnates as no new software can be deployed, forcing users to explore other solutions and for the operations staff to waste their time in fixing these problems.	High	New software releases will be rolled out to sites in stages restricting the sites exposed to any new software. Operations staff will also be involved in setting the performance and deployment environment for new components. Failures will be reviewed to see if improvements are needed in the assessment criteria, the work of the software provider or the overall process.

1.5.4   Work Package SA2: Provisioning the Software Infrastructure

1.5.4.1 Summary

Work package number	SA2		**Start date or starting event:**		1/5/2010		
Work package title	Provisioning the Software Infrastructure						
Activity type	SVC						
Participant number	1	9	10	12	16	21	29
Participant short name	EGI.eu	CESNET	KIT	CSIC	GRNET	INFN	LIP
Person-months per participant	36	95	24	71	95	47	71
Participant number	36	38					
Participant short name	UCPH	VR-SNIC	TOTAL				
Person-months per participant	24	24	487				

Objectives

This activity will coordinate the external provision of software required by EGI to form the production infrastructure. It will:

- Establish agreements with key software providers
- Maintain the UMD Roadmap
- Define general and component specific quality criteria to be applied to software components
- Verify the software components against these criteria
- Provide a repository for the software components within UMD and the related support tools
- Provided a distributed 'support unit' within the EGI Helpdesk infrastructure with expertise on the deployed middleware in production use

---

Description of work

TSA2.1: Activity Management

This task focuses on the management of the activity and the relationship with EGI's software providers. Prioritised requirements from elsewhere in EGI are collated and distributed to the current software providers and published for the whole community. The functional roadmaps and release dates from individual software providers are assembled into an integrated UMD Roadmap. The projected UMD Roadmap is monitored and the effectiveness of software providers to deliver components to the required schedule and quality will be reported to the MCB. This work will be managed by the CTO who reports to the Project Director and will hold regular meetings of the team to ensure effective coordination of its activities.
Requested Effort: 36PMs EGI.eu

TSA2.2: Definition of the UMD quality criteria

The generic component acceptance criteria will be provided and updated according to evolving needs. Specific criteria will be developed for components on the UMD Roadmap.
Requested Effort: 36PMs CSIC, 36PMs LIP

TSA2.3: Verification of conformance criteria

The components contributed to the repository will be validated against the generic and component specific conformance criteria. SA2 will be involved in pre-release component testing. Verification of each component will be summarised in an acceptance report, available with the component in the repository.
Requested Effort: 36PMs CSIC, 36PMs LIP

TSA2.4: Provision of a software repository and support tools

Necessary services to deliver the functionality of the repository and its surrounding process (FTP server, web server, issue tracker, version control system, etc.) will be provided and maintained.
Requested Effort: 48PMs CESNET, 96PMs GRNET