EGI Proposal

WP3 = SA1 – e-Infrastructure Operations

Draft 4c - 17/8/2009

Authors: John Gordon, David Kelsey, Jesus Marco de Lucas, Torsten Antoni

[Comments and questions for co-authors and the internal reviewers shown thus]

Version Log

#	*Authors*	*Description*
1	*JCG*	*Using the structure of the bidding document, list all the activities from the Blueprint and Functional Description that fall within these sub-activities [The BP and FD only list the various activities and say nothing about how they are managed so much of this document is new. One approach is to look for parallels in EGEE and see if they are still relevant in the EGI/NGI model]*
2	*JCG*	*Redrafted to use the structure from the FD*
3	*JCG, DPK, JML*	*Expanded to cover whole of SA1. Added drafts of WP3.4 and 3.5.* *Changed header depth to agree with Laura's overall SA draft.* *Haven't moved anything from 3.4 and 5 to a higher levels.*
4	*JCG*	*Removed extraneous WP3.5 notes.*
4c	*TA*	*Moved user support part to 1.5.1.4.2 and added content there* *Removed sections 1.5.1.4.1.6 and 1.5.1.4.1.7*

1. PLACEHOLDER

1.5 PLACEHOLDER

1.5.1 Activity SA1: e-Infrastructure Operations

1.5.1.1 Activity Summary

This draft covers WP3.2 e-Infrastructure Operations subsections:-*[I've claimed SA1 for this activity as it appears as the first SA in the outline proposal]*

SA1.1 WP Management tbd ; SA1.2 Operations Coordinationconsists of: the ownership of the standards that bind the NGIs together; the monitoring of the performance of the NGIs for International VOs; oversight of the global services with which the NGIs interact; and management of the issues arising from all of the above. *[In many subtasks I have described my assumptions about EGI's inheritance from EGEE III. These are to help with the scope of what migration work will still be needed in EGI. Those more knowledgeable than me should update them. Once we are happy with the programme of work etc, they can be removed from the final proposal JCG]* SA1.3 User Support Coordination (to be summarised) SA1.4 Operational Security Coordinationcovering the development and maintenance of security policy (O-E-15) and the coordination of security and incident response (O-E-16) within the NGIs (O-N-9a).

SA1.5 Operational Services - the global services run by specific NGIs on behalf of the whole project must be closely integrated with the work of the NGIs that interact with them. In some cases (eg accounting) the NGIs publishing data and the global repository receiving it are two parts of the one whole. In others (eg Coordination of middleware roll-out) there is no separate service, just the coordination of the work of the NGIs. Thus most of the work of the global tasks are covered in SA1.2 but there is another aspect of the quality of the global task delivery and compliance with the SLA which should be the subject of special scrutiny and management under this task.

1.5.1.2 Activity Management

Two sides to this:-

a) The usual activity management stuff of effort to WBS, quarterly reports, deliverables, milestones to be completed by an expert in a uniform manner for all activities.

b) The oversight of the sub-activities and the work of the NGIs and other service providers. *[In this area management and coordination overlap. For this draft I describe this bottom up below. Later we can pull a summary of the various bodies and roles that fall out into this section.]*

1.5.1.3 Activity Description

1.5.1.3.1 SA1.1 WP Management

1.5.1.3.2 SA1.2 Operations Coordination

The EGI Blueprint (ref) defines the various tasks that are performed centrally by EGI.eu, or by an NGI on its behalf, and the international tasks that all NGIs carry out in order to support cross-border working. The details of these are expanded in the EGI Functional Description (ref) and the numbering scheme from the latter is used through this section. *[The proposal should eventually have an appendix listing them]* The approach taken here is to discuss each separately or in small groups and then later to define the minimum number of coordination bodies to monitor performance effectively. These bodies will be under the overall coordination of this activity.

There are several levels of coordination required with different timescales.

a) Short-term – to deal with operational exceptions as seen by VOs. In theory all issues should get resolved by the support/helpdesk processes but we see that a meeting (real or virtual) provides good information flow and guarantees appropriate escalation. Examples include the WLCG Daily Operations Meeting and the EGEE Weekly Operations Meeting.

b) Oversight of the Sites – a hierarchy of teams monitoring the sites, raising tickets, providing support. A continuous process for continuous improvement of site and service reliability

c) SLA Review. Consideration of how sites and NGIs are performing in the medium to long term. Takes input from monitoring and from VOs

d) Individual service advisory groups. A meeting between service providers and stakeholders to review the performance over an extended period and propose changes to requirements, service levels, procedures, etc. *[Good working examples include USAG which brings together VOs and sites with GGUS, and GOCDB-AG which provides input to GOCDB developments. Consider whether we need one per service or if some can be combined]*

e) Development plans for Operations Tools. Takes input from (d) but has an integrated view of how the tools interwork and share infrastructure. Works with WP4.

f) Liaison of ‘operations’ with other activities.

For each of the above we need to define:

- Terms of Reference
- Membership *[A recurring issue as there will likely be too many NGIs for complete representation everywhere]*
- RACI and reporting lines.

Listing them all in the proposal might be overkill.

[Next step is to work on better definitions of the above.]

1.5.1.4 Description of the Tasks

[repeat for each BP task

- *One subtask for each ‘international task and/or global task’ from the BP/FD.*
- *Describe assumptions on the status by end of EGEE III*
- *Define proposed steady state (with NGI options)*
- *Roadmap/milestones to get there*
- *Note requirements for ongoing development assumed (cross reference to WP4)*
- *Proposal for oversight: advisory board, champion, etc*

]

1.5.1.4.1 SA1.2 Operations Coordination

1.5.1.4.1.1 SA1.2.1 O-E-1 and O-N-1: Operation of the Grid topology and configuration repositories

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 Grid repository provides all such information. Information input is devolved to regions and sites. The current central repository (known as GOCDB in EGEE) may need to be adapted to support a two-tier distributed model. This requires the definition and implementation of common interfaces and transport mechanisms to ensure the exchange of information between different Grid domains.

By the end of EGEE III, a new version of the current repository GOCDB will have been deployed to fill this role. It will run a central database containing a sub-database per EGEE region. These will be managed by the regions. The capability for the database to be deployed remotely in a ROC or NGI and to synchronise with the central instance will be possible but no assumptions are made about whether this is in use.

EGI is responsible for running the central service where other services can find information and maintaining the schema of the centrally-held information. This may be the master copy for an NGI, or a cached copy if the NGI runs its own service

The NGI is responsible for maintaining data about itself and its sites. If it runs its own repository, it is responsible for publishing the agreed schema to the central database.

Milestone 1: Plan for further distribution. Participating NGIs to decide how they manage their data. Do they wish their own instance, use a regional one, or a national/regional partition of the central database, managed by the region or NGI.

Milestone: 2: Implement Plan. Beyond this milestone, changes will be an operational issue negotiable between the NGI and the global service provider.

1.5.1.4.1.2 SA1.2.2 O-E-2 and O-N-2: Operation of accounting repositories for international VOs

The accounting repository is responsible of keeping records about usage of compute, storage, networking and other types of resources as required by the users, resource providers, NGIs, etc . It is the responsibility of a NGI to collect accounting data, and to keep a permanent master copy of usage records. Accounting information is needed by international VOs in order to allow VO managers to know about the amount of IT resources "consumed" by the respective users across different domains of the e-Infrastructure.

By the end of EGEE III, a new version of the APEL client will have been deployed using the ActiveMQ Message Bus. The NGIs which are already publishing from their own accounting solution in EGEE III will also have ported to this new transport layer. A version of the APEL Central Repository capable of being run independently by an NGI and publishing data into the central repository will have been developed and tested but it is not assumed that this has been deployed in production. The central APEL Repository which currently holds data on LHC and EGEE VOs can act as the default repository for international VOs.

EGI is responsible for running the central service where VOs can interrogate their usage, and maintaining the schema of the centrally-held information.

The NGI is responsible for maintaining data about all usage made of its sites and for publishing data on international VOs to the appropriate repository.

Milestone 3: Plan for further distribution. Participating NGIs to decide how they manage their data. Do they wish their own instance, use a regional one, or to continue to publish accounting data directly to the central service.

Milestone: 4: Implement Plan. Beyond this milestone, changes will be an operational issue, negotiable between the NGI and the global service provider.

1.5.1.4.1.3 SA1.2.3 O-E-3 and O-N-3: Operation of Grid repositories storing monitoring and performance data and other related information

Availability, status and performance information about Grid services and sites are needed to check the health of the infrastructure and to verify the Quality of Service delivered to VOs and other NGIs. Gathering and publication of monitoring information – regarding Grid functionality, Grid service status, assessment of quality of the services delivered by various EGI actors (resource providers, the NGIs, etc.) – is consequently important to help the infrastructure to assess its level of service and compare it to the VO requirements. This also requires the operation of repositories and supervision of the processes to populate them, the maintenance of schema for publishing of site and service status information, the ownership of the information schema used, the preparation of reports, etc.

It is assumed that all EGEE Regions and some NGIs will already be running their own Nagios monitoring infrastructure, and metric store. The data will also be published to a central metric store from which EGI-wide reporting will be possible. SAM tests will no longer be run centrally from CERN and tools which interrogated the SAM database will have been ported to use the metric store. It is also assumed that existing ROCs will continue to run monitoring for the relevant NGIs until at least milestone 6 has been passed.

EGI responsibilities are the publication of statistics, the maintenance of schema for central publication of site and service status information, the deployment of monitoring-related tools such as the dashboard and the alarm system, and the preparation of performance reports.

NGI responsibilities are to monitor their sites, make the information available through a local portal and publish information to a central metric store.

Milestone 5: Plan to devolve Nagios testing from regions to countries where required.

Milestone 6: implement plan.

1.5.1.4.1.4 SA1.2.4 O-E-4 and O-N-4: Operation of the Grid Operations Portals

The Grid operations portals provide an entry point for various actors to support their operational needs. Different "views" are necessary according to the role of the customer (Grid operators, VOs, Grid site managers, Region Operations Managers, etc.). The information displayed is retrieved from several distributed sources (databases, Grid information systems, etc). It provides static information about sites/VOs, and dynamic information about resources/services status and allocation. The central Operations portal is the aggregation point of regional information, which is also accessible via regional operations portals.

By the end of EGEE III a version of the CIC portal will be maintained centrally with the management distributed to regions and VOs. The first milestone will be to increase the granularity to NGIs to allow NGIs to maintain their information in the central instance. NGIs will also be able to interface a national repository of this information with the central repository.

EGI responsibility will be to run the central portal and automate gathering of the required information

NGI responsibility will be to maintain relevant information about their infrastructure and VOs.

Milestone 7: Delegate responsibility to NGIs where and when appropriate

1.5.1.4.1.5 SA1.2.5 O-E-5 and O-N-5 Grid operation and oversight of the e-Infrastructure

At the core of this task is the monitoring and support of the sites through a ticketing system which will contain issues raised as a result of SLA checking (i.e. SAM monitoring tickets or equivalent), VOs, users and system administrators. This ensures that the International VO's get the services agreed through EGI. The practical work needed includes:

- Monitoring and help desk shifts
- Triage of incoming problems, assignment of tickets to the 2nd line support units, ticket escalation to EGI.eu, 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 SLA.
- 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 global EGI.eu ticketing system

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. This is covered by O-N-3.

It is assumed that an NGI will be operating a ticketing system to coordinate its own national activities. Effort is needed to interface this national system into the EGI.eu system so that tickets can be exchanged and easily escalated (for example, those opened locally can be passed to the central instance or other areas, while user and operational problem tickets can be open centrally and subsequently routed to the NGI local support infrastructures). Interfacing the national help desk into the central help desk is the responsibility of the NGI, which will be supported by the central help desk staff.

1.5.1.4.1.6 SA1.2.8 O-E-9 Coordination of middleware roll-out and deployment, middleware pilot and certification testbeds

Comment [jcg1]: Needs a description of task

It is important to ensure that middleware updates move from certification and into production as quickly as possible, while also assuring that the updates are suitable for deployment in the production Grid. EGI.eu coordination will be needed for strategy decision, for example to decide significant changes to processes, and to ensure that resource sites are encouraged to upgrade whenever new critical updates of supported middleware stacks are released. Being still in a phase where middleware is subject to frequent bug fixing cycles, prompt alignment of the Grid services and components to the latest releases, contributes to better functionality and availability of the overall infrastructure.

1.5.1.4.1.7 SA1.2.9 O-E-10 Coordination of resource allocation and brokering support for VOs from NGIs

VOs can specify requirements in terms of resources to be guaranteed by the overall pan-European Grid infrastructure used. In this case, coordination – as required by VOs – contributes to ensure that a suitable production infrastructure (Grid core services and resources offered) is in place, to meet such requirements. Development is still needed to provide tools for the automation of the management and the negotiation of SLAs.

EGI is responsible for support and coordination of this process.

1.5.1.4.1.8 SA1.2.10 O-E-11 Coordination of interoperations between NGIs and with other Grids

Coordination is needed to foster the creation of a seamless operations model across administrative boundaries, in order to pursue pervasiveness and sustainability of the infrastructure. This is of great importance as users who want to cross Grid boundaries need to know that the environments will be similar, and applications must function properly without major changes. Interoperation covers a number of aspects, such as the availability of common tests for monitoring of site status, the interconnection between helpdesks/ticketing systems, etc. “Other Grids” includes Asia-Pacific regional Grids, OSG, Naregi, and related infrastructure projects.

This role owns the definition of the operational tools interfaces, the procedures and the operational activities allowing the NGIs to interoperate. EGI aims at continuing the collaboration established with operations centres outside Europe in order to preserve the current integration of non-European sites into the production infrastructure. EGI.eu is responsible for support and coordination.

1.5.1.4.1.9 SA1.2.11 O-E-12 Coordination of network support

Network operation design, handling of troubles affecting international VOs, and network assessment allow EGI to keep the state of the network under control, and to establish link between Grid operations and network operations. A centralized approach is proposed here in order to keep this task is close relationship with the other External Liaison tasks run by EGI.eu.

1.5.1.4.1.10 SA1.2.12 O-E-13 Definition of best practices, operations procedures, operations requirements

Interoperation relies on the definition of best practices and of general operational procedures for daily monitoring activity for sites and federations.

EGI.eu is responsible for the coordination of these activities.

1.5.1.4.1.11 SA1.2.13 O-E-14 and O-N-8: Operation of the production Grid Core Software Services,

catch-all services for international VOs, catch-all VO

Grid core services are components of the EGI e-Infrastructure. They are software components that typically run on server machines. With Grid service we refer to a software instance (a Web service in many cases) "that is designed to operate in a Grid environment, and meets the requirements of the Grid(s) in which it participates." [GLO]

In particular, Core Software Services are those necessary components provided by the Middleware Consortia on which the overall Grid functionality relies in order to operate. Catch-all instances can be required to support small user communities. It is a responsibility of EGI.eu to ensure that user communities are properly supported by the NGIs of reference. 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.

1.5.1.4.2 SA1.3 User Support Coordination

1.5.1.4.2.1 SA1.2.6 O-E-6, O-E-7 and O-N-6, O-N-7: central and regional Grid user support and ticketing system

User support relies on a central helpdesk, which is a regional support system with central coordination [GGUS]. It gives access to user documentation and support, and to a ticketing system. The central system is interfaced to a variety of other ticketing systems at the NGI level in order to allow a bi-directional exchange of tickets (for example, those opened locally can be passed to the central instance or other areas, while user and operational problem tickets can be open centrally and subsequently routed to the NGI local support infrastructures).

Support to network end-to-end problems in the Grid is also important – especially for applications requiring high-availability – as connectivity is provided by the pan-European network research backbone and by a large number of National Research and Education Networks, each providing links to sites within countries. A Network Operation Centre provides the operational interface between the Grid and the relevant network players to check the end to end connectivity of Grid sites [ENOC].

The NGIs provide 1st line local/regional support to users and centres, while EGI.eu takes care of the Maintenance and Operation of the central ticketing system (GGUS like) and of the Triage of incoming problems.

a. Maintenance and Operation: run a central ticket handling system for Grid and network end-to-end problems. User support relies on a central helpdesk, which is a regional support system with central coordination [GGUS]. It gives access to user documentation and support, and to a problem ticketing system. We expect only a fraction of the NGIs to be ready, at the beginning of the project, to fully run their national support infrastructure and integrate it with the central EGI tools. Therefore the effort used to enable NGIs interconnecting their support infrastructure with the central one will be spread over the whole project, especially as some partners will enter the project later.

b. Triage of tickets entering the central user support system (also known as ticket processing management in EGEE), consists of the monitoring and routing of all active tickets in the Grid user support system by Grid and VO experts, who are responsible of addressing the problems to the appropriate second-line specialized support units. This process combines manual as well as automated procedures. This task has more aspects than just the triage of incoming problems, as most of these will be directly assigned to the respective responsible support units. The monitoring of the overall workflow and the escalation of unresolved issues will be the more important and more time consuming part of this task. The members of the first line support team should divide their time between this task and other operations tasks, this way enabling them to build up the knowledge they need to successfully perform this task.

1.5.1.4.2.2 SA1.2.7 O-E-8 Gathering of requirements for user support tools and process

Tools and the process for user support are designed to meet the requirements of customers taking input from NGIs, VOs and resource centres. Additional requirements may arise with the evolution of the middleware stacks in use, and with the support of new user communities.

This task is crucial for the success of the overall user support infrastructure. It consists of chairing a user support advisory group that should be manned by all stakeholders and customers of user support. The management of this group is located in operations, but the scope and membership of the group should cover the whole project.

This group should not only gather requirements from users and providers of services, tools and software, but also define the overall support infrastructure of EGI in a way the will be most beneficial for the users and at the same time least disruptive for the providers of support.

EGI.eu is responsible of the coordination of this process.

1.5.1.4.3 SA1.4 Operational Security Coordination

There are many important challenges to be addressed in the area of computer and network security for EGI. Today’s public networks are a hostile environment, where sites and systems connected to them are under constant attack. The collaboration of a large number of independent sites in one e-Infrastructure potentially amplifies the security problems. Not only do these infrastructures contain large computing and data storage resources connected by high-speed networks, these being very attractive to potential attackers, but the connectivity and ease of use of the services means that a successful compromise of one site can threaten the e-Infrastructure in general and all of the participating sites.

The aim of EGI Operational Security is to address the various risks involved and to maintain the availability of EGI services. In spite of all best efforts, vulnerabilities will be found in the software deployed and security incidents will happen. All of these must be promptly and efficiently handled.

Agreed common Security Policies are required to regulate the activities of all participants: NGIs, resource providers and user communities alike. These common policies will facilitate the use of resources by user communities in any NGI willing to support them and also encourage interoperability between EGI, the NGIs and other infrastructures elsewhere.

A common authentication trust domain is required to persistently identify all Grid participants. To ensure interoperability, both at the European as well as the global scale, the project will participate in and collaborate with the International Grid Trust Federation (IGTF), and the EUGridPMA in particular, in line with the relevant e-IRG recommendations.

All operational and policy-related security activities are part of task WP3.4. The main activities include:

a) The coordination of all aspects of operational security, including response to security incidents;
b) The development and maintenance of the EGI Security Policies;

c) The handling of security vulnerabilities in the middleware and deployment;

d) Collaboration with the International Grid Trust Federation, its federated identity trust domain, and the integration with other national or community based authentication-authorisation schemes;

e) Overall coordination of all Security activities both within EGI and with other infrastructures.

1.5.1.4.3.1 Operational Security Coordination (EGI CSIRT)

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.

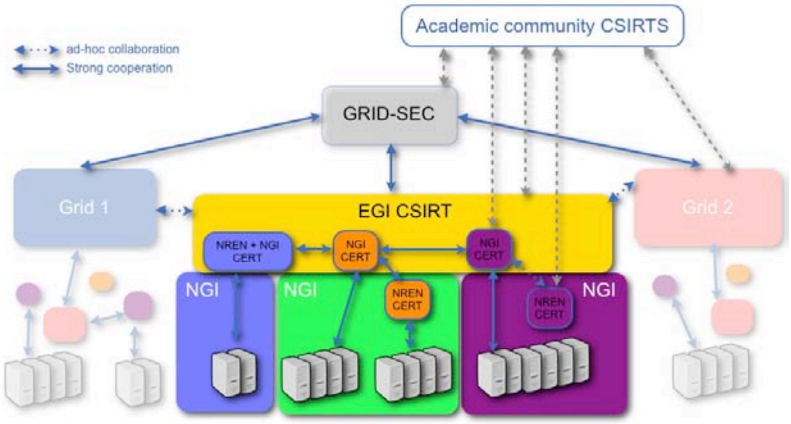
1.5.1.4.3.1.1 EGI CSIRT strategy

It is essential to ensure a coherent and comprehensive collaboration, at the operational security level, between all the resource providers of the EGI user community.

As security incidents may affect any resource providers, inside or outside EGI, the appropriate procedures, information flow and a collaboration based on trust have to be implemented to ensure security incidents are dealt with appropriately by the resource providers and the involved CSIRTs.

The large number of resource providers and the infrastructure topology requires a structured approach to be adopted, based on the different levels. From bottom to top:

- Site CSIRT (hundreds, usually one per site)
- NGI CSIRT, NREN CSIRT (tens, the degree of interaction between NGI and NREN CSIRT varies)
- Main academic grid CSIRT (units)



As a result, the EGI CSIRT ensures both the coordination with peer grids (via its GRID-SEC membership), and with the NGIs and NREN CSIRTs.

1.5.1.4.3.1.2 EGI CSIRT mission

The main objective of the EGI CSIRT is to provide the EGI infrastructure with incident response capabilities across the participating NGIs.

By implementing a number of procedures, technical means and appropriate communication channels, the EGI CSIRT ensures that that all incidents are investigated as fully as possible and that sites promptly report intrusions. In particular, security incidents are to be treated as serious matters and their investigation must be resourced appropriately.

In addition, the EGI CSIRT acts as a forum to mutualise efforts and resources from the NGIs in different areas:

- Grid security monitoring
- Security training and dissemination
- Incident response improvement (e.g. security drills)

1.5.1.4.3.1.3 EGI CSIRT regulation

The activities and mandate of the EGI CSIRT are regulated by the EGI security policies, developed and maintained by the JSPG and adopted by EGI. Additional security procedures will be implemented and agreed by EGI via the appropriate approval process.

1.5.1.4.3.1.4 EGI CSIRT membership

Each NGI appoints a "NGI Security Officer" (post O-N-9a) in order to provide the NGI CSIRT function:

- Coordinate the security activities within the NGI
- Ensure the coordination of the resolution of security incidents in the NGI
- Contribute to the EGI CSIRT
- Act as a contact point for security issues in the NGI for the rest of the infrastructure
- Participate in the other EGI operational security groups as necessary

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 (post O-E-16), whose role and mission are defined by security policies approved by EGI and the NGIs.

1.5.1.4.3.2 Security Policy Group (SPG)

The Security Policy Group (SPG) is responsible for the development and maintenance of security policies and for providing advice on any security policy issue. This will be led and coordinated by EGI (post O-E-15).

SPG's primary stake-holders will be internal to EGI, i.e. the NGIs, the sites and the application communities. Building on the earlier work within the Joint (EGEE/WLCG) Security Policy Group, SPG will continue to aim for common simple policies for interoperation across the world. Participation in SPG by policy experts from other e-Infrastructures will therefore still be encouraged. New policies will be submitted to the IPG (a body providing high-level alignment between the major infrastructures) for discussion and feedback.

The membership of SPG must contain not just representatives from the NGIs, but also some Site managers, VO managers, middleware experts, operations experts, operational security experts etc. Policy document revisions and new documents will be prepared by a small(ish) editorial team, which will do much of its work during face to face meetings. SPG will also maintain a much larger mailing list of all interested stakeholders for wider consultation of new policies. This larger body is unlikely to be able to hold face to face meetings, except perhaps during EGI conferences, and business will be done by e-mail or phone conference.

As before in JSPG (EGEE-III), the SPG policy will supplement local NGI policy, not replace it. EGI policy should be the small set of general common rules and responsibilities to allow NGIs to interoperate, and more importantly allow international user communities to easily use resources across EGI, and indeed across the world.

It will be important to consult widely with Sites and VOs during policy development, not just NGIs (NGIs should lead this consultation within their country). Formal adoption of policy should be by a suitable policy board (EGI Council?) and not SPG itself, otherwise SPG will become too political and this will stifle policy innovation.

SPG will not just prepare and maintain formal policy documents. Security policy input will be required in many other bodies. The Policy coordinator (O-E-15) or other SPG members will represent EGI security policy interests on IGTF, EUGridPMA in particular, TERENA and NREN federations activities and other groups, such as the Software Security Group. New security middleware components, particularly in the area of Authorisation, will be developed and made available to EGI by UMD. It will be important that appropriate operational security and security policy input is provided to discussions on these to ensure that they meet the needs of EGI and the NGIs and that deployment can be achieved while achieving interoperable services.

1.5.1.4.3.3 Software Vulnerabilities Group (SVG)

In EGI it will be important to ensure that the Grid software and deployment is as secure and free from vulnerabilities as possible. The main purpose of the Software Vulnerabilities Group is to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, and prevent the introduction of new ones. The aim is to prevent Grid security incidents.

In EGI, middleware will be distributed as part of the Unified Middleware Distribution (UMD). The SVG will be part of the EGI Security Operations but will also need to interact strongly with development teams and the UMD co-ordination. SVG will draw members from both the operational teams and development teams, but 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.

1.5.1.4.3.3.1 Vulnerability Handling

A simple method whereby anyone can report a potential Grid Security Vulnerability issue found in the UMD distribution or the deployed infrastructure and be confident that the issue is investigated and handled in an appropriate manner will be needed. The method will largely be based on what has been established in EGEE-III, with changes according to both lessons learnt and the EGI setup. The principle should remain that:

- Anyone can report an issue
- The Risk Assessment Team (RAT) carries out an investigation and Risk Assessment.
- A Target Date (TD) is set according to the Risk.
- An advisory is provided when the issue is resolved or on the Target Date, whichever is the sooner. This is considered to be 'responsible disclosure'.

The most important aspect of the GSVG issue handling is to provide a risk assessment, so that issues can be appropriately prioritized and fixed in a timely manner. Reporting to SVG ensures that issues can be kept private while they are investigated and if appropriate fixed in a timely manner.

In EGI the SVG will need to have defined contact points with each software provider from which the software is built. There also needs to be an expectation of turnaround time in response to the report of a vulnerability concerning that software, along with agreement that the Grid Security Vulnerability issue handling process will be applied to that software along with the responsible disclosure strategy. These should be part of the MoU with the provider. Additionally, if software providers find and fix vulnerabilities in their own software they should agree to provide the patched versions to the UMD and co-ordinate the release of patches and advisories with UMD/EGI.

The SVG leader (a potential NGI International Role?), along with 2-3 deputies, will co-ordinate the running of the process. These will be supplied by various NGIs. A number of RAT members will also need to be supplied from the development teams, the NGI site administrators and deployment teams, or other security experts. This group of people will establish the exact methods and criteria for carrying out the handling process. This will both encourage people to join in with the process so that they can help establish the criteria, and provide a broad acceptance of the criteria across EGI.

This central SVG issue handling process will also ensure a reasonable degree of uniformity of the Risk Assessment and issue handling process across EGI.

1.5.1.4.3.3.2 Code security assessment and Developer training

As well as handling specific vulnerabilities found, it is important to actively check that the deployed middleware is secure. This could be done by NGI volunteers developing the expertise to assess code for vulnerabilities. Or it could involve invitations to external experts to find vulnerabilities, including possible peer recognition for those finding the most serious vulnerabilities.

1.5.1.4.3.3.3 Developer Training

There is an education role for SVG within the developer community to improve the quality of the deployed software that also needs to be fulfilled. It is important to ensure developers are educated in secure and defensive coding in order to prevent the introduction of new vulnerabilities.

1.5.1.4.3.4 IGTF and EUGridPMA support and participation

A common authentication trust domain is required to persistently identify all EGI participants. To ensure interoperability, both at the European as well as the global scale, the project will participate and support the International Grid Trust Federation (IGTF), and the EUGridPMA in particular, in line with the relevant e-IRG recommendations. Leveraging the previous investments of EGEE in this effort, and building on successful new initiatives using national federated identities for the Grid, it is in the interest of EGI to ensure that the EUGridPMA can continue to fulfil this role in the identity federation.

This sub-task will also coordinate the provision of EGI versions of the IGTF Certification Authority distributions, as EGI will wish to have the ability to add or remove authorities as specified by the project. NGIs may also want to add more (national or training) CAs, or even remove specific CAs that are incompatible with national policy. In these cases, such an NGI will need to build its own distribution locally so it may be better to distribute this task either immediately or after year 1 of EGI.

1.5.1.4.3.5 Overall coordination of EGI security activities

Information exchange will need to happen between the various operational sub-tasks described above. NGI Security Officers and their local teams will also need to be well informed of developments happening in areas in which they are not directly involved. This could be achieved by annual face-to-face meetings of all security groups, for example at the EGI Conference. Information mail lists may also be used for the receipt of quarterly reports from each group and for discussion of general issues.

EGEE-III had a Security Coordination Group, consisting of the chairs of each of the sub-groups, which met monthly by phone. Perhaps we should continue this in EGI?

1.5.1.4.3.6 Effort evaluation

This needs to be consistent with the other tasks in WP3, so no table is completed here.

The two EGI posts are

O-E-15: Security policy development and maintenance to define agreement on best practice and security policies, CA policies (EUgridPMA) etc. (EGI.ORG + NGI). A team of security people in NGI's will take care of ensuring the definition and application of standard security policies - EGI.org support and coordination.

O-E-16: Coordination of security and incident response (EGI.ORG + NGI) – the EGI Security Officer - in the region for NGI and overall for EGI.org to ensure that common policies are followed for coordinated incident response by grid participants- EGI.org coordination and support.

NGI effort for task WP3.4 is part of O-N-9 (Operations Coordination), specifically sub-task O-N-9a (Security Incident Response): The NGI Security Officer - Security incident response, security policy, periodic security challenges to test the national/regional readiness, collaboration with the NREN for security matters, etc. This is extra effort on top of existing national staff resources.

Other (volunteer) effort from NGIs and/or NRENs will be needed for SPG, SVG and IGTF.

1.5.1.4.3.7 Milestones and Deliverables for WP3.4

Still to be provided.

1.5.1.4.4 WP3.5 SA1.5 Operational Services

1.5.1.4.4.1 Activity summary

All the tasks previously described in this section require a combination of central and NGI-distributed services. The objective of the task 3.5 is to assure the deployment and operation of these services on the corresponding infrastructure. The list of services includes:

1) Grid topology and configuration repositories.

2) Grid Operations Portal

3) Monitoring and performance data repositories

4) Production core software services

5) Accounting repositories for Global Virtual Organizations

6) Ticketing system and document repository for support

1.5.1.4.4.2 Activity management

As indicated the services will support the activity of the previous tasks, and the management will be correspondingly articulated. However the deployment and operation of the services in the adequate infrastructure will be undertaken by a small number of partners with well defined SLAs.

1.5.1.4.4.3 Activity description

Description of each subtask

1.5.1.4.4.3.1 SA1..5.1) Grid topology and configuration repositories

The Grid topology and configuration repositories provide information on the service nodes, contact details, certification status and down-time status. Gathering and making available the configuration information for each NGI will be done via a central repository. The definition and implementation of an exchange protocol between peer NGIs will be also addressed.

1.5.1.4.4.3.2 SA1.5.2) Grid Operations Portal

TBD

1.5.1.4.4.3.3 SA1..5.3) Monitoring and performance data repositories

The subtask will take care of the publication of monitoring information regarding Grid functionality, Grid services status and an assessment of the quality of the services delivered by resource providers, and in particular by NGIs. This information is critical to meet the agreed level of service. The subtask will detail the operation of the repositories, supervise the processes to populate them, maintain the schema used for publishing the site and service status information, and also contribute in the preparation of reports.

1.5.1.4.4.3.4 SA1..5.4) Production core software services

This subtask will address the operation of catch-all production grid core services, the catch-all services for global Virtual Organizations, and the catch-all Certification Authority.

1.5.1.4.4.3.5 SA1.5.5) Accounting repositories for Global Virtual Organizations

The subtask covers the operation of Grid accounting repositories, required for Global Virtual Organizations in order to make this information available to the Virtual Organization managers so they can have an overview of the resources used across the different domains of the e-Infrastructure (EGI.org + NGI). It will require gathering and making publicly available the accounting information (as applicable and according to local laws) for each NGI.

1.5.1.4.4.3.6 SA1.5.6) Ticketing system and document repository for support

The central ticket handling system for Grid and network end-to-end problems will be operated within this subtask. User support is based on GGUS (Global Grid User Support), a central helpdesk configured as a regional support system with central coordination. It gives access to user documentation and support and to a problem ticketing system. The first level and regional support will be provided through the NGIs.

1.5.1.4.4.4 First overview of the milestones and deliverables

DSA1.5.1 EGI Operations Infrastructure Services Description , M6 (type: Software + Report)

MSA1.5.1 Release of the Infrastructure Services in Operation at EGI.org +NGI level, M6, DSA1.5.2 Analysis of the Use of Infrastructure Global Services and the Coordination with NGIs, M12 (type: Report)

MSA1.5.2 Full integration of all NGIs in EGI.org Operations Infrastructure, M18

DSA1.5.3 Satisfaction level with Operations Infrastructure for User Support, M21 (type: enquiry + report)

DSA1.5.4 Integration of Operations Infrastructure Services at World Level M24 (type: report)

DSA1.5.5 Global Experience New possibilities for Operations Infrastructure Services M33 (type: report)

1.5.1.4.4.5 Overview of the risks and the contingency plan

TBD

1.5.1.4.4.6 Contracts

Defining and monitoring the contracts/SLA between EGI.eu and the NGIs tasked with delivering them. The selection of NGIs to carry out these tasks will be done by EGI before the start of the core EGI project but since to start with the funding will be predominantly from the EC this should be a task in the core proposal.

1.5.1.4.4.7 Quality

The definition of metrics and the measurement should be an objective duty of this task although more subjective input should also be obtained from the NGIs and the relevant Advisory Groups defined in SA1.2

1.5.1.4.5 Milestones and Deliverables

[Define these in the task descriptions for now. Gather together here later]

1.5.1.4.6 Overview of the risks and of the contingency plan

The best case scenario is that EGEE III ends with an operational model already deployed independently in all EGEE regions and capable of easily being deployed by NGIs instead of regions. The non-EGEE communities get integrated smoothly with the relevant NGIs The risks all involve the alternative scenarios:

- Not enough NGIs join EGI to cover all the countries needed by the international VOs.
- EGEE Operational Services do not make enough progress towards distribution before the end of EGEE III. Too much further development of tools required in EGI leading to an unbalanced profile.
- Working practices do not scale to number of NGIs. Working groups inefficient due to size.
- NGIs all deploy alternative services leading to overwork of staff of global counterparts in supporting NGIs interfacing

Mitigation involves existing ROCs continuing to support other NGIs until they are capable of taking on distributed services for themselves. NGIs grouping together to achieve critical mass and expertise. Model of representation so that all NGIs don’t have to participate in all operational bodies.