Summary of EGI-InSPIRE PY1 Review –WP4

The EGI-InSPIRE PY1 Project Review took place in Amsterdam on June 30 and July 01; the technical review report was received on the 5th of August. This document provides information about the technical comments that concern WP4 (Operations) and a summary of the future work recommendations.

The overall assessment of the progress is "Good (the project has achieved most of its objectives and technical goals with minor deviations)" and the technical work carried out was rated "highly commendable". As to WP4, the main area of comment is security and risk assessment (see following section).

The project review provided feedback on the activity during PY1 and proposed changes to the work plan for future years. These proposals are currently under review by the project management.

Progress of the WP4 work package

[EGI-InSPIRE Technical Review Report, pag 19]

The objectives of WP4 for the current period have been achieved. Technically, the work carried out in WP4 is well managed, very well led, and is of a consistently high quality, meeting the goals, milestones and objectives described in the DoW but with delays. The progress made in WP4 for this reporting period is in line with that planned in the DoW. Resource consumption has been rather erratic but is expected to be brought under control in the next period. The current deliverables were made available sufficiently on time to the reviewers. All partners involved in this work are deploying their skills cohesively and have performed well.

The objectives associated with WP4 for the coming period, as described in the DoW, are still relevant with respect to the state of the art and are still achievable within the time available to the project but would benefit from having a **coherent long-term business strategy** to fit within (see section 1c).

SA1 is by far the largest Work Package in the project; it is larger than all of the others put together. The work carried out in this Work Package includes security accounting and infrastructure management.

The EGI resource infrastructure is based on the building blocks of Resource Centres which are organised into a resource infrastructure and this is managed by an NGI. The many NGI resource infrastructures were decomposed and extended out of the legacy regional grid organisations created in EGEE. NGIs contribute their resource infrastructure to the EGI. EGI.eu coordinates the provision of the technologies and services which the resource infrastructures consume. The relationships between EGI.eu and the Resource Infrastructures and the technology providers are provisioned through SLAs.

The EGI service infrastructure is composed of: infrastructure services, technical services, support services, and human services.

- Infrastructure services assist the end users to access and manage grid resource infrastructures. MyEGI GUI, which was started in EGEE, was completed in the first year of EGI and deployed. An access portal, a help desk, communication and accounting services were also deployed.

- Technical services operate over the resource infrastructure to assist the deployment and integration of new technologies. These include requirements gathering, staging software roll out, ensuring interoperability and providing core middleware services.
- Support services help users to get onto the grid and to stay there if they want to, mainly through help desks but also through dissemination activities and training courses.
- Human services collect and assess project metrics, negotiate and manage SLAs, keep the infrastructure safe, document the work carried out and manage operations.

During the first year, minor issues were experienced by SA1 but these were overcome with relative ease.

Security measures are in place beyond the technical FPVA[1] methodology and are reported in the EGI milestones rather than deliverables. There seems to be a tendency to **focus almost exclusively on threats to technical vulnerabilities**. While it is gratifying, indeed, that security is being taken seriously in EGI, the current focus may well be too tight. It is a mature but very conventional risk-assessment based technical software system security model.

Grids present a particularly complex threat surface and **(non-technical) system vulnerabilities** may well go completely unobserved, unless a comprehensive approach is taken. Has the question: "What does it mean to be secure in a grid" been asked? Given sufficient resources and time, a grid infrastructure could be rendered secure in the fullest sense, this is very likely not possible in other more highly virtualised environments and represents one of the key grid differentiators. **The delivery of D4.4 in M19 offers the opportunity to initiate this investigation and discussion**.

The plans for the coming year are sensible and achievable.

Recommendations concerning the period under review for SA1

Rec. 6. Security

Consider a ground up security review for grid infrastructures in general and EGI in particular. Start from the question: "what does it mean to be secure (trusted, private, controlled, etc.) in the grid? Remember that people are part of a grid. Consider the results from a verification point of view: can the grid infrastructure offer security assurances in the context **of systems accreditation** to conduct a range of sensitive services that meet both **commercial and regulatory requirements**? Work is underway in the ISO 27000 community to try to resolve these types of problem.

Recommendations concerning future work for SA1

SA1 to support existing users

Combine NA2 and NA3 to provide the resources for the recommendations which follow and which focus on acquiring new user communities, strengthening the strategic planning activities, and designing and deploying the strategic metrics. SA1 to take care of existing users.

[1] First Principles Vulnerability Assessment