EGI-InSPIRE

SECURITY RISK ASSESSMENT OF THE EGI INFRASTRUCTURE

EU DELIVERABLE: D4.4

Document identifier:	EGI-SCG-D44-863-v1_0
Date:	**17/01/2012**
Activity:	**SA1**
Lead Partner:	**STFC**
Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/863

Abstract

This document reviews security in the European Grid Infrastructure (EGI). It describes the scope and aims of EGI security, including the assets that EGI security seeks to protect. The work of the various security groups in or associated with EGI is briefly described. Practices and standards for IT security and their usage and possible future usage are described. Some security incidents have occurred over the last year, these are briefly described including how they were handled. Previous Overall Security Risk assessments are then summarized, and plans for a security risk assessment which will take place over the following months is described.

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Dr Linda Cornwall	STFC	
Reviewed by	**Moderator:** **Reviewers:** <<To be completed by project office on submission to AMB/PMB>>		
Approved by	**AMB & PMB** <<To be completed by project office on submission to EC>>		

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
0.1	19th August 2011	TOC and strategy notes for discussion	Dr Linda Cornwall, STFC.
0.2	24th August 2011	Additions and modification after discussion on review recommendations	Dr Linda Cornwall, STFC.
0.3	15th September 2011	Revised after finding the actual assessment need not be done until later, only description in D4.4	Dr Linda Cornwall, STFC.
0.4	18th October 2011	Added 1st draft of text for sections 2,3, and 4	Dr Linda Cornwall, STFC.
0.5	3rd November 2011	Minor changes from Peter Solagna's comments	Dr Linda Cornwall, STFC
0.6	15th November 2011	Some additions and restructuring from discussions on 9th November, including sections allocated for various people's completion	Dr Linda Cornwall, STFC

0.7	24th November 2011	Added input from various people (Riccardo Brunetti, David Groep, Maarten Litmaath, Mingchao Ma, Giuseppe Misurelli). Added some more sections.	Dr Linda Cornwall, STFC
0.8	6th December 2011	Input/addressed comments from Dave Kelsey, Oscar Koeroo and Tiziana Ferrari	Dr Linda Cornwall, STFC
0.9	9th December 2011	Added diagram. Added section 6.4 as suggested by Peter Solagna. Added exec summary	Dr Linda Cornwall, STFC
1	22th December 2011	Addressed Dave Kelsey's and most of Tiziana's comments. Referencing tidied and removed 'in-line' links.	Dr Linda Cornwall, STFC
1.3	17th January 2012	Partially addressed reviewers comments – asking for input from some others before fully addressing	Dr Linda Cornwall, STFC
2			
3			

IV. APPLICATION AREA

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

V. DOCUMENT AMENDMENT PROCEDURE

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

VI. TERMINOLOGY

A complete project glossary is provided at the following page: http://www.egi.eu/about/glossary/.
Additional glossary items relevant to this document are below

DoW	EGI Description of Work
FPVA	First Principles Vulnerability Assessment
ISMS	Information Security Management System
ISO	The International Organization for standards

VII. PROJECT SUMMARY

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

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

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

The objectives of the project are:

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

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

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

VIII. EXECUTIVE SUMMARY

This document reviews security in the European Grid Infrastructure, and presents a plan for a security risk assessment of EGI.

In the first section we present our answer to the question "what does it mean to be secure on the grid?" and "what assurances can we give users, resource providers, and others?" This includes a description of the aims of EGI security including what users and Resource Providers should expect. It describes the different types of data handled on the Grid, including making it clear that the Grid is not suitable for the handling of financial data. EGI's role and responsibility and limitations are described. EGIs assets, which need to be protected, are categorized.

The various security groups and their roles in EGI are summarized.

Some various practices and standards for information security are described. Usage of some of these in the Grid environment is also described, along with the experience of having used these. This includes some of the EGI procedures which are partially based on standards, including some aspects of EGI security incident handling. Some examples of usage of technological standards in EGI are also described. Possible future uses of standards are also described.

The operational security work carried out since the start of EGI is summarized.

A plan for a security threat risk assessment is described, and previous risk assessments are briefly referred to. The plan is to select threats to EGI's security, and where possible define which asset or assets each threat refers to. The risk is then computed. Traditional computation of risk, e.g. by insurance companies, is the actuarial computation of risk based on statistical values of likelihood and cost. In the EGI environment we do not have suitable statistics, so a strategy has to be defined in their absence. In this case we base risk on a judgement by the members of the EGI security assessment team on the likelihood and impact, and this is used to compute risk. The current mitigation in place, which for some threats will include activities currently carried out by the various security groups, in EGI will be considered. Recommendations will be made on the need to keep current activities in place and any new mitigating action needed.

The plan to carry out this risk assessment during the first quarter of 2012 is described, along with some estimations of the amount of effort needed.

Security risk assessment is an on-going activity, something that is never complete. It is necessary to re-do and revise risk assessments from time to time, as the situation is constantly changing and new threats emerge. As well as carrying out a Risk Assessment in early 2012 we recommend repeating it around 18 months later, towards the end of 2013, to enable any remaining High risks to be addressed before the end of the EGI-InSPIRE project.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 From the EGI-InSPIRE DoW

In the EGI-InSPIRE Description of work (DoW) [R 1] D4.4 is described as "A comprehensive review will be undertaken of the current EGI Production Infrastructure to assess its security vulnerabilities and associated risks. This 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."

1.2 From the EGI-InSPIRE Year 1 review

Recommendation 7:

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.

Additionally, in the SA1 comments:

Security measures are in place beyond the technical FPVA 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.

1.3 Content of D4.4

This D4.4 Security review describes more than just a review of the technology, as described in the DoW, but a more comprehensive review of security in the Grid environment. This document includes the following:

- A description of 'Scope and Aims of EGI Security'. This is our answer to the question 'What does it mean to be secure in the Grid'.
- A brief description of the security groups in EGI and the work currently undertaken by these groups.
- A look at practices and standards, including the ISO27000 series and their applicability to the Grid infrastructure.
- A summary of operational security and of the type of security incidents that have occurred since the start of EGI, and how they have been dealt with.
- A plan for a security Threat Risk assessment. This will describe the strategy for carrying out this assessment of security threats to the Grid, but the assessment will be carried out over the following months and be reviewed periodically.

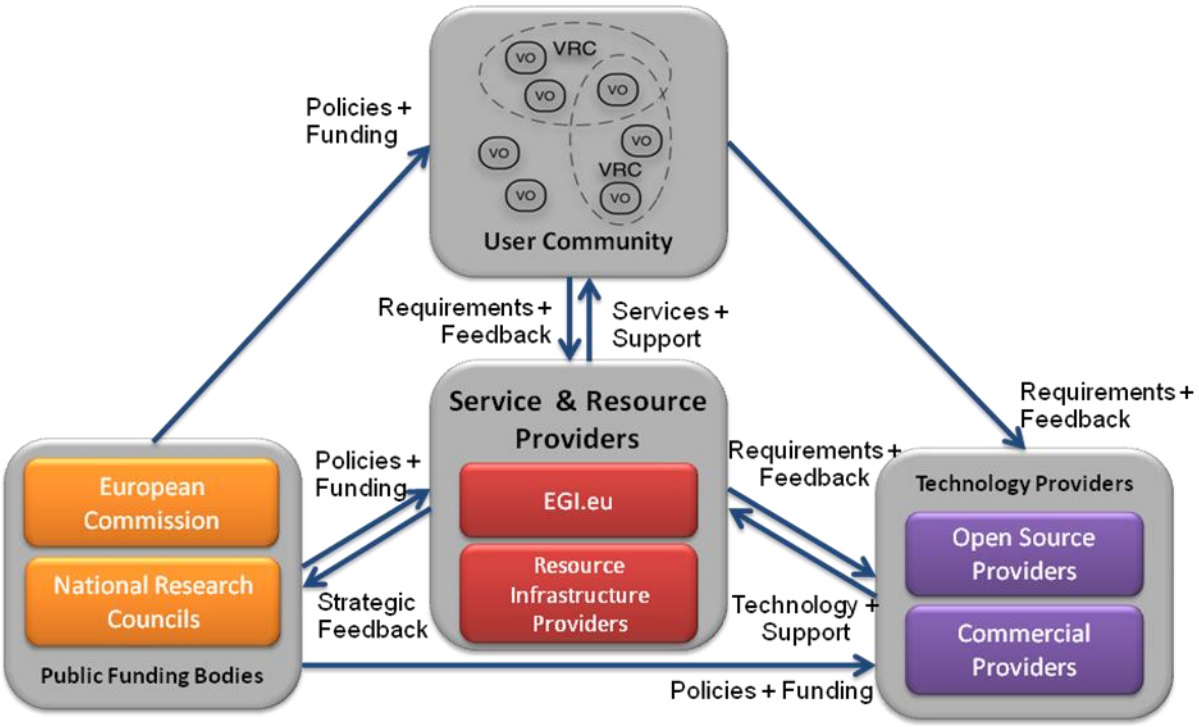
Review of EGI security is an on-going process, and is never completed. On-going activities include the reviewing of procedures, addition of new procedures needed, and the carrying out of Security Risk Assessments.

2 SCOPE AND AIMS OF EGI SECURITY

In this section we present our answer to the questions, "what does it mean to be secure on the grid?", and "what assurances can we give to users, resource providers and others?" This section describes the EGI ecosystem and assets which need to be protected by the various EGI security policies, procedures and mechanisms. This then goes on to describe what users, resource providers and others can expect. Section 3 briefly describes the groups and activities in EGI whose activities help to provide these assurances.

2.1 The EGI Ecosystem

2.1.1 Diagram of the EGI Ecosystem



The EGI Ecosystem consists of all components that make up or interact with EGI. This includes Services and Resource Providers (RPs), EGI.eu, Users, Technology Providers, and the funding agencies.

2.1.2 Public Funding Bodies

Most of the funding that allows the EGI to operate comes directly from Public Funding bodies: the European Commission and the various National Research Councils.

2.1.3 Service and Resource Providers

EGI.eu provides various services that enable the coordination of the production infrastructure which help the production infrastructure to function. The Resource Providers (RPs) provide most of the actual physical Grid infrastructure including the people to operate and manage the infrastructure and are members of the various National Grid Infrastructures (NGIs). Some services and resources (such as training) are provided by both EGI.eu and the RPs.

2.1.4 Technology Providers

Technology providers supply the technology which enables the infrastructure to function. Some of these are commercial, such as the providers of hardware and operating systems. Some (mainly Grid Middleware providers) are other publicly funded activities such as the European Middleware Initiative, (EMI), the Initiative for Globus in Europe (IGE), Simple APIs for Grid Applications (SAGA) with which EGI.eu has a service level agreement.

2.1.5 User Community

The User community uses the resources provided in order to carry out their work. These are mainly in the form of computing resources to process and store data in order to carry out their work. Users are members of Virtual Organisations and it is as a result of their proven identity and membership of Virtual Organisations that they are granted access to the resources they wish to use.

2.2 EGI's Assets

Assets may be defined as any resource or capability. Often these are given a financial value, to consider for example the value of a company. Security can be seen as the protection of assets. Some of EGI's assets are intangible, such as EGI's reputation.

Most of EGI's assets are not owned by EGI.eu, but are necessary to make EGI work and deliver a service to users. A monetary value is not placed on the assets, even though a cost is associated with providing them and keeping them available. This document does not consider how to keep the assets in place through funding, but confines itself to considering the security threats to the assets.

2.2.1 Management

The high level interactions with various communities, funding, training, and management is carried out by EGI.eu. This also includes strategies for sustainability and business models to ensure that the distributed computing resources are available to the research communities in the future.

Management also occurs in various other places, such as within NGIs, individual Resource Providers, and within various Virtual Organisations.

2.2.2 Organization

EGI relies on widespread organization to keep everything working together. This includes the GGUS ticketing system for answering queries, with a wide range of people available to call to resolve different problems. It relies on the GOCDB, the database of NGIs and RPs to keep up to date information on the Infrastructure, so appropriate people can be contacted when necessary.

Access to the Resources is governed by membership of a Virtual Organization (VO). A VO refers to a dynamic set of individuals or institutions defined around a set of resource sharing rules and conditions. A typical VO in the EGI context is a group of people working in geographically different locations in a particular scientific research area. Users are members of one or more VOs. For each VO they are a

member of they may also be a member of various groups within the VO and have certain roles within each VO. Resource Providers give access to their Resources based on membership, groups and roles of various VOs.

Authentication credentials are provided by identity providers including Certification Authorities which are members of the International Grid Trust Federation as in section 3.5.1

Both users and resources need to be authenticated.

VO managers decide who is a member of their particular VO and what rights they have, as well as providing authorisation credentials to users to prove their rights.

Some RPs run VO membership services for a VO allowing it to concentrate on the management of their membership without having the responsibility of running the actual services.

2.2.3 Process

Various processes are defined within EGI. For example, there is a process for obtaining credentials for use in the EGI environment. The various security groups have procedures for handling certain situations, such as incidents. There are processes which are carried out to join the production infrastructure.

2.2.4 Knowledge

The web pages (including Wiki) provide information for users, sites, and others about how EGI is run operationally. This includes procedures to follow, e.g. how should a site become part of the grid, how a site should handle a security incident, to training materials for users, and information on events.

In order to gain knowledge Training needs to be provided. Training for various people who interact with the grid is provided by various sources. For example security training for site administrators is largely provided by CSIRT (see section 3.3). Training for users is also provided by both manuals and courses provided. Some training is provided by the NGIs whereas other training is provided by the various partners.

Support is provided (based on authentication using identity credentials) via the Global Grid User Support (GGUS) system for users and others who interact with the Grid.

2.2.5 Information and Data

The main purpose of EGIs existence is the storage and processing of data and information for its scientific user communities. Such data and information needs to be stored reliably and owners of data must be able to rely on the integrity of the data. Owners also need to be able to rely on being able to access the data, yet it must not be possible for the data to be accessed, modified, or deleted except according to agreed access rights. Owners and those with agreed rights also need to be able to process data, using CPU in the hardware available on the Grid.

Data may belong to VOs or individual users, and this is stored and processed on the various hardware resources provided by Resource providers. It is the storage and processing of data which is at the heart of the purpose of the EGI infrastructure and Ecosystem.

2.2.6 Software and Applications

Provisioning the Software Infrastructure which is essential for EGI to function is an activity carried out by the EGI-InSPIRE project, as WP5 (SA2). Various recommended software installations and configurations are available to the RPs. Information on how to obtain appropriate software can be found from the EGI website. The software which enables the sharing of resources is distributed by the EGI Unified Middleware Distribution (UMD), and is built upon the Linux operating system. EGI itself develops very little software (the exception being operational tools) but recommends and re-distributes

software, including that provided by external projects such as the European Middleware Initiative (EMI) and the Initiative for Globus in Europe (IGE) with which EGI has a service level agreement.

Various software applications are also used by users belonging to the various VOs on the Grid.

Software comes into many categories, from the operating systems, to Grid Middleware which enables the safe sharing of resources on a large scale, to software used by users and VOs to process their data. Software integrity is just as important as data integrity. It is important that software behaves as it should and processes data in the intended manner and does not contain vulnerabilities or malware.

2.2.7 Infrastructure

The Resource Centres (RCs) are members of the various National Grid Infrastructures (NGIs). The RPs provide the computing resources that constitute the National Grid Infrastructures. This includes the hardware, installing and configuring the software which enables the sharing of resources in a distributed infrastructure, proving their identity, allowing members of various VOs to have access to their resources, ensuring their security and complying with agreed policies. The Operation of the various RPs is largely co-ordinated by the EGI-InSPIRE project as WP4 (SA1). Resource providers have access to training on how to run a secure site, as well as help when they need it.

The hardware provided by the various Resource Providers, although not owned by EGI.eu, forms the main Physical infrastructure of EGI.

The infrastructure also includes the network that connects everything together. This is largely owned by 3rd parties and shared with others other than EGI.

2.2.8 National Grid Infrastructures

National Grid Infrastructures (NGIs) manage and co-ordinate work at national level. There are 39 NGIs spanning Europe, the Far East, Canada and Latin America. The NGIs apply for funding both from the EU and their national funding bodies, contribute people, and fund resources in the EGI infrastructure.

2.2.9 People

No organisation can run without people. Any organisation depends on appropriate personnel to carry out the various task needed to make things work. People are an asset to EGI.eu. Whether they are employed by the Resource Centres to run and maintain resources, whether by NGIs or partners to provide training or support to users, or whether employed in the overall management of EGI.

Users may be seen as an asset, if they ceased to use EGI then funding would quickly end and there would be no EGI.

Users obtain credentials to be used in authentication, for example from a Certification Authority which is a member of the International Grid Trust Federation as in section 3.5.1

They register with Virtual Organisations they are members of, and the VO provides them with authorization to carry out actions in the Grid. As part of the process of joining a VO users also sign an Acceptable Use Policy, whereby they agree to abide by EGIs rules.

After obtaining appropriate credentials users may interact with and use the resources to which they are entitled on the Grid. Users also have access to various documentation and training resources.

2.2.10 Financial Capital

All the various activities which form the EGI ecosystem need funding. This is true whether the funding comes from the EC via the EGI-InSPIRE project, from national funding agencies or other sources. The funding and people's willingness to keep funding the EGI Ecosystem is largely dependent on EGI being seen as deliver to its user communities and whether people feel it is worth

continuing to contribute to this infrastructure. In order for funding to continue those who decide on funding need to be confident that EGI will deliver the resources reliably and securely for their users, and that the benefit and efficiency of EGI is worth the cost of providing and maintaining the widely distributed computing infrastructure.

2.2.11 EGI's reputation

EGIs reputation depends on those contributing funding to the infrastructure and its users being happy with the service they are getting. This includes a steady improvement in the service available, to at least match emerging technologies in the wider world. EGIs reputation could very quickly be damaged if there were to be an incident leading to a large loss of data, or if the EGI infrastructure were to be used to carry out a major cyber attack on other systems.

2.3 Aims and Role of EGI.eu

2.3.1 Aims of EGI Security

The EGI home web page states "The European Grid Infrastructure enables access to computing resources for European researchers from all fields of science, from High Energy Physics to Humanities." EGI aims to provide users with open access to computing resources including data storage on its production infrastructure, in order to carry out their work. The purpose of security is often seen as to allow people the benefits to which they are entitled.

EGI security is aimed at the safe integration of and access to distributed resources in the production infrastructure.

Some (but by no means all) aspects of traditional approaches to security are not appropriate in the EGI environment, as they are aimed at preventing widespread access to resources, because all assets lie within a single management domain. EGI is designed to allow widespread access, as do cloud service providers. Within the EGI environment a wide user base is encouraged to access the resources and there are many different management domains. The resources which constitute the EGI, for example, are managed by the various Resource infrastructure Providers (RPs) and as such EGI.eu has no direct control. The best we can achieve is to define a very clear security policy framework and implement procedures that all participants have to follow. If security incidents happen EGI needs to have robust procedures to deal with these including the exclusion of a failing RP or other participant if necessary to contain the effects of the incident.

Some aspects of a more traditional approach to security are still appropriate, such as encouraging RPs to adopt and follow best practice in the management of their resources. Similarly many conventional tools for managing security, for example encryption of data, usage of checklists are deployed in the Grid.

2.3.2 EGI.eu's Role

EGI.eu's role is to coordinate with NGIs, Resource Providers, Virtual Research Communities, EUGridPMA [R 9] and other stakeholders to ensure that the production infrastructure is as secure as is practical. To tackle this complex problem space EGI.eu has many security activities working in parallel: Policies (SPG), Procedures (CSIRT and SA1), Software Vulnerability handling (SVG), Operational Security (CSIRT, Incident Response etc), Security Drills, Security monitoring, Security training (to encourage best practice). EGI also initiates any activities that are regarded as necessary to deal with Security Threats that may be identified.

2.3.3 EGI.eu's responsibility

EGI.eu's responsibility includes leading collaboration with the stakeholders mentioned above, to put appropriate controls in place, and to jointly implement procedures to aim for smooth and secure running of the EGI. This includes ensuring that the technology which enables the sharing of resources in its infrastructure is as secure as is practical. This includes software distributed by EGI.eu or recommended by EGI.eu for installation by RPs and RCs. EGI.eu also encourages RPs, RC's Users, and others who interact with the Grid to follow best practice.

EGI.eu's responsibility is also finite. The production infrastructure is not a single management domain and as such EGI.eu has no direct control of the resources provided by the RPs, RCs and NGIs. EGI.eu establishes policies and procedures on behalf of the community which requires NGIs and RCs to implement secure operations as this is important for the security of operation of whole of EGI, but EGI.eu cannot be held responsible for the RCs actions. RCs are also responsible for playing their part in security incident handling. EGI has an agreed incident handling procedure which they are expected to follow and members of the EGI CSIRT Team are often able to help, but EGI has limited access to the RCs log files, and RPs will need to do most of the work themselves. Similarly, it is the responsibility of individual RCs to take care of local physical security, such as access to their machine room and fire prevention. Again all of this is required by EGI security policies.

EGI cannot ever guarantee security, but should do what it can to mitigate common risks, help RPs and RCs mitigate risks, and encourage others to mitigate risks from identified threats.

2.4 Users and EGI security

2.4.1 What assurances can users expect?

Users can expect a system that is Suitable for use. This includes:

- Convenient access to Resources
- Data and information security is appropriate
- Confident they cannot accidentally damage system
- Cannot be liable for unintentional actions that cause problems including excessive usage of resources
- Cannot be liable for actions for which they are not responsible

This largely means that the security in place needs to allow appropriate access and prevent problems.

2.4.2 What assurances can users NOT expect?

Users cannot expect a perfect or perfectly secure system, or guarantees. This includes:

- Guarantees that resources will always be available
- Guarantees that data can never be read by others, such as system administrators
- That their usage of resources is confidential

2.4.3 Obligations of Users

Users need to take care of their credentials and take care when using the system. This includes:

- Being aware and complying with the acceptable use policy
- Protecting their certificates
- Taking care not to leave a session logged in without locking the computer

2.5 Resource Providers and EGI security

2.5.1 What assurances can Resource Providers expect?

Resource Providers need to be confident that by becoming a part of the EGI infrastructure will not cause security problems at their sites. This includes:

- The mechanisms and technology enabling the Grid do not lead to insecure sites
- The mechanisms and technology enabling the Gird do not lead to damage to their sites
- The mechanisms and technology do not allow access beyond intended rights such as to other resources on the sites.
- Being part of the Grid does not damage their reputation.
- RPs and Resource Centres (RCs) need to be confident that they receive appropriate support in the secure deployment of the Grid technology,
- They cannot be legally liable for actions carried out by others, such as unlawful use of copyright software or other illegal activities carried out on their resources

2.5.2 What assurances can Resource Providers NOT expect?

Resource providers cannot expect the mechanisms and technology to be perfect, or that there will never be problems.

2.5.3 Obligations of Resource Providers

Resource providers are obliged to carry out certain actions to maintain security. These include:

- Configuring their sites in a secure way
- Keeping their software up to date
- Maintaining physical security, such as access to the machine room
- Reporting an incidents, and participating in their investigation

2.6 Data and Information Security

2.6.1 Personal identity and accounting data

Delegated proxies are currently stored widely in the infrastructure, and are generally accessible to system administrators. This does not necessarily mean that system administrators can impersonate users, as some software uses "limited proxies" on the final job destinations that can't be delegated further, which this limits the ability of malicious administrator to submit new jobs. This will still give the administrator access to data. However, there may still be cases where system administrators need to be trusted not to impersonate users.

Long lived proxies are stored in MyProxy servers, which have carefully controlled access, and facilitates the renewal of proxies used for long lived jobs.

Accounting data is also stored in the infrastructure. Computing Elements retain job records in files that typically are accessible only to service administrators. Users who are allowed to access a particular Computing Element currently may have access to some aspects of its accounting information. Accounting records are regularly uploaded to the EGI central accounting repository that implements very strict access control rules to protect the privacy of users, while providing details to site, NGI and VO managers in accordance with the EGI policy on accounting data. This policy defines the framework and responsibilities for the management, transmission, storage of and access to user-level accounting data.

2.6.2 General Scientific data

Users need to be sure that their data is stored reliably, has integrity, and is available for access. This means that appropriate procedures need to be in place to ensure that data is stored reliably, and cannot be tampered with. This includes for example backing up data and/or storing it in more than one place.

Data backups and the storage of multiple replicas (and backup is a case of replication to the offline medium) leads to a wider attack surface the replicated data, so security procedures should be deployed for these operations.

Access control needs to be in place, which allows access to data according to defined access control for that specific data. Appropriate access control according to the application is needed. In some cases data should only be readable by a single user; in others it may be readable by a group of users. It is common for data to be readable by members of the same VO. In some applications at present where data is not sensitive (at least for the LCG VOs) the vast majority of the data is available to anyone who is authenticated and is a member of any VO that is supported by the storage element in question. This is because the usual permissions allow "others" to read the files. This may be appropriate for some scientific data, but for other data it is not appropriate.

Scientific data is generally stored in an unencrypted form. Site administrators can generally access all data stored on the services for which they are responsible.

2.6.3 Other Scientific Data

In addition to the concerns above certain applications, e.g. biomedical, need to keep their data confidential. If such confidentiality is needed it is the responsibility of the applications to store the data in encrypted form and manage the encryption keys. Encrypted data and decryption keys shouldn't be stored together on the same persistent storage at a site. This so that if the site is compromised it is not possible to extract bulk encrypted data from the persistent storage and the appropriate keys to decrypt it. It should also not be possible for site administrators to decrypt bulk encrypted data stored on their site. However when data is decrypted for processing it is readable by the site administrators. This also implies the proper cleaning of work areas on the data processing devices, since naively removing the temporary decrypted data leads to the situation where it can be restored without much effort by the site administrators or attackers that gained access to the computing field of the site.

2.6.4 Sensitive Financial Data

EGI as an organisation does not store or process any sensitive financial information or data, such as credit card details, nor has it been designed to do so. Similarly, the International Grid Trust Federation (IGTF) [R 2] minimum requirements and assurance level do not specify any guarantees with regards to liability for the identity management system. Although there are no technical limitations prohibiting the infrastructure from dealing with sensitive financial data, there is no accompanying policy and liability framework to allow appropriate processing of such data. This applies both for the underlying identity management systems as well as for the EGI security policies and procedures. This does not prevent users storing public financial information, such as current stock prices, on the EGI infrastructure.

2.6.5 Other Data

<<David Groep Improve/expand.>>

The EGI infrastructure is not suitable for the storage and processing of certain other types of data. This includes any data where the real time or near real time storing and retrieval of the data is vital, such as

safety critical data. The EGI infrastructure is also not generally suitable for highly sensitive data, such as defence related, or large databases of personal data.

3 SECURITY GROUPS AND ACTIVITIES IN EGI

This section summarizes the various security groups in and related to EGI, and how they interact. Each group's activity complements the others and the whole is essential for the proper management of risk to EGI's assets. Each group carries out activities which aim to make the Grid secure enough to mitigate the identified risks.

3.1 The EGI Security Policy Group

The **Security Policy Group (SPG)** is responsible for developing and maintaining the Security Policy for use by the NGIs. This policy defines the expected behaviour of NGIs, RPs, Users and other participants, required to facilitate the operation of a secure and trustworthy distributed computing infrastructure.

More information is available from the SPG Wiki page at [R 4]

Procedures are developed by EGI security groups and other operational bodies to implement the overall security policies.

3.2 The EGI Software Vulnerability Group

The goal of the **Software Vulnerability Group (SVG)** is to eliminate existing software vulnerabilities from the deployed infrastructure and prevent the introduction of new ones, thus reducing the likelihood of security incidents.

The largest part of the activity is the handling of specific vulnerabilities reported to the SVG. The SVG also co-ordinates with other groups and software providers to define priorities and a timetable for the assessment of software used in the EGI infrastructure for vulnerabilities and the education of developers and packagers to prevent the introduction of vulnerabilities.

A summary of the main tasks of the SVG is available [R 5] and more details are available from the SVG Wiki [R 6]

3.3 The EGI Computer Security Incident Response Team

The **EGI Computer Security and Incident Response Team (EGI CSIRT)** is a security team aimed at coordinating the operational security activities in the infrastructure, in particular the response to security incidents. The EGI CSIRT carries out the coordination with the NGIs and if applicable with NREN CSIRTs and security teams of peer grids. 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.

A description of the main tasks of the EGI CSIRT team is available [R 7] and more details are on the public wiki [R 8]

3.4 The EGI Security Co-ordination Group

The **Security Coordination Group (SCG)** brings together representatives of the various security functions within the EGI to provide coordination between the operational security, the security policy governing the use of the production infrastructure and the technology providers whose software is used within the production infrastructure. Membership consists of the chairs of the SPG, SVG, CSIRT, representatives from the EUGridPMA, EMI and IGE Security Teams (i.e. technology providers), and the EGI.eu Chief Operations Officer and EGI.eu Director.

3.5 Related Groups

3.5.1 The EU Grid PMA and International Grid Trust Federation

The EUGridPMA is the international organisation to coordinate the trust fabric for e-Science authentication in Europe, and a member of the International Grid Trust Federation IGTF to ensure global coordination of trusted identities for e-Infrastructures. The various country-based and regional identity providers (who for the purposes of working with the Grid infrastructure issue PKI certificates to users and resources) are members of the EUGridPMA or its peers in the Asia Pacific (APGridPMA) and the Americas (TAGPMA). The certificates issued by such authorities are accepted as identification in the EGI. EGI is represented in the EUGridPMA through a dedicated liaison function, alongside other members including the issuing authorities and relying parties. More information is available at the EUGridPMA website [R 9].

3.5.2 Software Security in EMI

Much of the middleware deployed within EGI is produced by the European Middleware Initiative, EMI. The EMI security area produces middleware services and components that enforce the Grid Security Model, allowing the safe sharing of resources on a large scale. These cover identity management, Virtual Organisation membership management, authentication, delegation and renewal of credentials, and authorization.

More information on EMI is available from their website [R 10].

3.5.3 Software Security in IGE

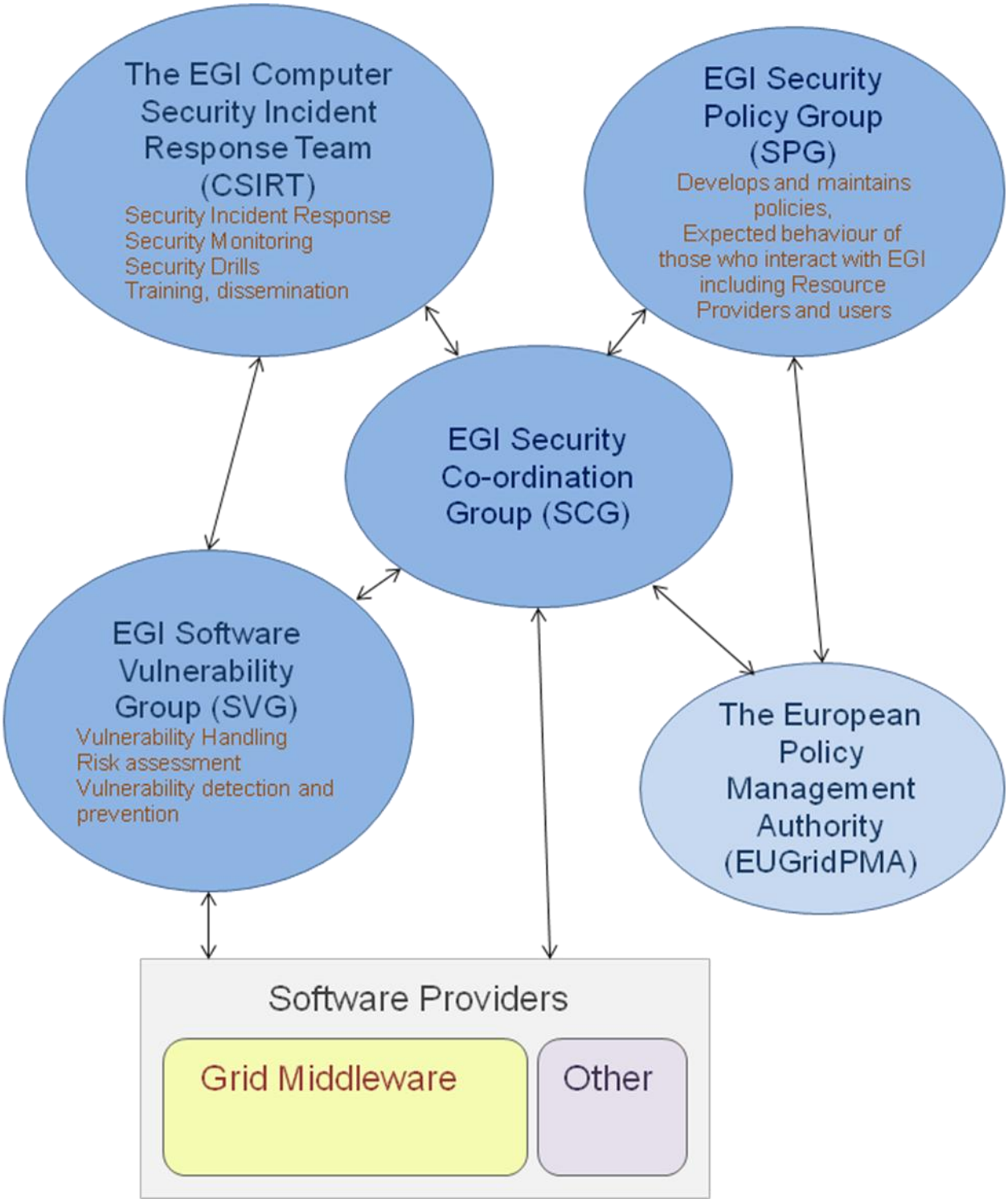
The Initiative for Globus in Europe (IGE) is the European project for Globus-based middleware. Due to the well-established legacy of services, tools, libraries and its protocols Globus is used as a foundation to various middleware solutions. IGE supports the Globus middleware from a European perspective by being in close contact with the US-based Globus development teams and providing solutions required by European-based user groups. Besides the Grid and HTC based communities IGE will also facilitate the support for HPC Infrastructure user communities from DEISA and PRACE with the Globus core services and user centric software solutions.

Furthermore IGE is facilitating a bridge between the Globus software developments and the emerging EGI driven requirements towards a sustainable infrastructure. IGE will manage the adoption and integration of the tools, technology and protocols which are required to be seamlessly integrated in the EGI ecosystem.

IGE will fulfil the role as security contact and coordinator for all the Globus tools, libraries, middleware, services and protocols. For more information on IGE, see [R 11].

3.6 Diagram of relationships between groups and main interactions

Note that all groups interact at some time and work together to produce a secure infrastructure.



4 PRACTICES AND STANDARDS

This section reviews the practices carried out by EGI in the security area, various standards, and whether it is appropriate and applicable to apply standards or practices in EGI which are not currently carried out. EGI is aware of Information Security best practices, and good practices are generally adopted and carried out where seen appropriate.

4.1 Standards for information management

4.1.1 ISO standards

The International Standards Organisation (ISO) [R 12] develops standards in various areas. The ISO 27000 series [R 13] of standards concern information technology, security techniques and information security management systems. The three published standards in this area are ISO 27001 (2005) Requirements, ISO 27002 (2005) Code of practice for information security management, and ISO 27005 (2011) Information security Risk Management, as well as ISO 27000 (2009) Overview and vocabulary.

It should be noted that ISO standards need to be purchased, they are not available free of charge, and the mechanism for purchase for our use (whether it is possible to have an 'EGI' copy, or whether individuals need their own) is not clear. The cost is not trivial.

4.1.2 NIST Standards

In the US the National Institute of Standards and Technology (NIST) [R 14] is an agency of the US Department of Commerce. The NIST publication SP 800-53 is entitled 'Information Security' [R 15]. The PDF of this is available for free download (237 pages long).

Alongside the NIST Standard, NIST has produced FIPS199, Standards for Security Categorization of Federal Information and Information Systems [R 16] which categorizes sites according to impact of loss of confidentiality, integrity and availability. FIPS200, the Minimum Security Requirement for Federal Information and Information Systems [R 17] describes requirements for each of these categories.

4.2 Examples of Application of Information management Standards in the Grid Environment

4.2.1 Example of ISO27000 standard used in EGI

ISO 27002-2005 was looked at by the Swiss Multi-Science Computing Grid (SMSCG), which forms the backbone infrastructure of the Swiss Grid activities. A Security Questionnaire for Infrastructure providers was produced based on this standard. This is available from the SMSCG information for site administrators. [R 18] This questionnaire consists of 32 questions which sites were expected to answer to ascertain whether their security was adequate. This included questions such as "Has the site implemented a Local Security Policy? Do you have revocation procedures (checklist) when people (staff) leave your institution? It refers to various checklists. This list was produced as a result of approximately 2 person weeks of work, from reading the ISO 270002 standard.

4.2.2 Example of NIST standard used in Grid environment

In the US, Grid infrastructure providers in national laboratories managed by the US Department of Energy were obliged to have their systems audited according to NIST standards. Even though their

systems fell into the lowest category according to the NIST standard FIPS199 [R 16] it was a major undertaking to produce the material needed, documented evidence and practice document for the audit took approximately 1 person year per site.

Members of Open Science Grid (OSG) consortium at the Stanford Linear Accelerator Center carried out a mapping of the NIST SP800-53 in 2007, identifying those section which are relevant for distributed infrastructures and Grid identity management operations (however this is not available publicly) when viewed from an trust interoperability point. Whilst providing a firm basis for security analysis, providing the documentary evidence in a form suitable for auditing against this subset of criteria remains a substantial effort which is only valuable if the results are actually reviewed by infrastructure peers.

4.2.3 EGI Procedures partially based on standards

<< Giuseppe Misurelli to address reviewers comments>>

From an implementation viewpoint, good practices defined in ISO27001/27002 can be seen as the achievement of a series of control objectives, thus resulting in a more pragmatic approach for an Information Security Management System (ISMS) based on ISO standards.

Among the overall objectives, and relative controls for each of them, listed into ISO27001/27002, a number of crucial ones can be applied to the EGI operations security area while others have been indirectly implemented in the past on the frameworks of policy and procedures defined within the different EGI working groups.

Notwithstanding, the possibility to adopt such standards in the EGI ecosystem is always bounded to the exploration and finding of convergences between control objectives suggested by ISO and the distributed nature of the community and infrastructure co-ordinated by EGI.eu.

Consequently, it is worth comparing a number of EGI procedures that are consistent with some of the aforementioned control objectives listed in ISO27001 Annex A, referenced in the following sections with the ISO nomenclature (A. plus the control number).

A.5 Security policy

A.5.1 Information security policy

ISO control objective: *Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*

ISO annex	ISO subject	ISO control	EGI implementation	EGI reference
A.5.1.1	Information security policy document	Document approved by management and communicated to all relevant parties	Policy documents are defined, approved by the EGI executive board and formally adopted by EGI community	https://wiki.egi.eu/wiki/SPG:Documents
A.5.1.2	Review of the information security policy	Documents shall be reviewed at planned intervals or if significant changes occur	EGI SPG reviews policies according to SPG internal procedures	https://wiki.egi.eu/wiki/SPG

A.10 Communication and operations management

A.10.1 Operational procedures and responsibilities

ISO Control objective: *Ensure the correct and secure operation of information processing facilities.*

ISO annex	ISO subject	ISO control	EGI implementation	EGI reference
A.10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained and made	EGI wiki as the main container of operation	https://wiki.egi.eu/wiki/Documentation https://wiki.egi.eu/wiki/EGI_CSIRT:Policies

	available to all users who need them	procedures, guidelines, roles and responsibilities	

A.13 Information security events

A.13.1 Reporting information security events and weaknesses

ISO Control objective: *Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.*

ISO annex	ISO subject	ISO control	EGI implementation	EGI reference
A.13.1.1	Reporting information security incidents	Information security events shall be reported through appropriate management channels as quick as possible	Incident response guide and operation procedures to report security incidents for the infrastructure and to establish well known point of contact.	https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts http://helpdesk.egi.eu/

A.13.2 Management of information security incidents and improvements

ISO Control objective: *To ensure a consistent and effective approach is applied to the management of information security incidents*

ISO annex	ISO subject	ISO control	EGI implementation	EGI reference
A.13.2.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents	Monitoring of services availability, alerts and vulnerabilities are constantly used to detect incidents in agreement with general and security operation procedures	https://wiki.egi.eu/wiki/EGI_CSIRT:Monitoring https://wiki.egi.eu/wiki/Grid_operations_oversight

Even if observed convergences cannot be addressed for an ordinary ISO certification purpose, some EGI procedures adhere to the implementation guidance behind the aforementioned control objectives especially for what concern information security procedures.

Nevertheless, in pursuing the integration of such implementation guidance, key control objectives on assets management should be taken into account in the framework of existing and future EGI procedures.

A.7 Asset management

A7.1 Responsibility for assets

ISO control objective: *Achieve and maintain appropriate protection of organizational assets.*

ISO annex	ISO subject	ISO control	Implementation guidance
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets draw up and maintained	Type of assets to be categorized. Information: databases, contracts and agreements, system doc, manuals, training materials, procedures, archives. Services: tools used by the EGI community and operated directly or indirectly by EGI
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designed part of the	Ownership as responsibility to ensure assets are properly classified, periodically reviewed in agreement with applicable

		organization	access control policies to update access restrictions and classifications

A7.2 Information classification
ISO control objective: *Ensure that information receives an appropriate level of protection*

ISO annex	ISO subject	ISO control	Implementation guidance
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization	Balancing the needs for sharing or restricting taking into account confidentiality, integrity and availability of the assets. Initial classification and future reclassification regulated by access control policy and carried out by asset owners
A.7.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization	Labelling should reflect the classification according to the guidelines in A.7.2.1. Handling procedures shall include the secure processing, storage, transmission an declassification of assets

Finally, implementing an EGI asset inventory can be considered as the source of data for a risk assessment and treatment in agreement respectively with a standard security risks management and an approved Risk Treatment Plan (RTP).

4.3 EGI's Use of Technology Standards

Technological standards are important for the secure interoperability between non-uniform infrastructures and reduce the likelihood of security problems. Several members of the EGI community are also involved in the development of security standards for use in the distributed computing environment, e.g. in OGF.

4.3.1 Grid middleware usage of standards

Many components of the Security Middleware used in EGI use or follow standards. For example, in EMI a SAML profile is used to describe attributes and X.509/SAML assertions are used to verify users' credentials. The Authorization policy language is an XACML based profile.

<< Riccardo Brunetti to expand/address reviewer's comments >>

4.3.2 Other examples of technology based on standards

There are other examples of technologies and instruments that are used in the day to day operations in the grid environment which are actually based on international standards. Just a couple of examples:

The AES (Advanced Encryption Standard) works behind the scene in almost all the secure communication that occurs when using the grid infrastructure. It has been announced by the NIST as an official U.S. FIPS 197 on November 2001.

The FIPS 140-2 standard, defining the requirements for physical and operational security of the HSM (Hardware Security Modules) has been announced on 2001.

It can be used (sometimes is requested by some EUGridPMA profiles) by root Certification Authorities to perform the key management and the signing operations on X509 certificates.

4.4 Possible future usage of and changes to practices due to application of standards

4.4.1 Threat identification

In the security assessment described in section 6 checklists based on standards will be looked through to see whether we have missed any important threats.

4.4.2 Threat mitigation and checklists

When the security assessment has been completed some threat mitigation may be based on standards, or more probably checklists based on standards. One possible source is the Sans Institute, which has produced various checklists on Information Security. These appear to be available for use free of charge, but are likely to have restrictions on use which EGI would have to adhere to. Some checks are appropriate on a per site basis, some may be appropriate in a wider EGI context.

4.4.3 Detailed examination of ISO27000 standards

The appropriate ISO27000 standards are foreseen to be examined in detail to decide their relevance to EGI. This may include the production of checklists and/or questionnaires for Resource providers, to help them maintain security.

4.4.4 EGI's relationship with the ISO standards community

EGI has no special relationship with the ISO standards community. No members of EGI are instrumental in producing these standards, and it is unlikely that the manpower is available to change this and provide input in the immediate future.

4.5 Conclusions on standards and EGI

4.5.1 Practices in EGI

The larger Resource Centres such as the Tier 1 centres are generally experienced in managing systems, and sites are likely to be mostly well managed. Such centres tend to have good practices in place, whether or not they are formally based on standards. Some of the smaller centres may be variable in terms of how experienced their system managers are. EGI policies and procedures are available to resource centres to help them with their security. If sites fail to follow appropriate procedures, for example by not installing an update to deal with a critical vulnerability they may be suspended from the production infrastructure.

Resource Centres may also have to conform to standards or practices in their own institution, or national standards depending on where they are located.

4.5.2 Formal accreditation

Formal accreditation is very costly; the effort involved in preparing a site for formal accreditation is considerable and the cost prohibitive. If formal accreditation were to be required e.g. for regulatory requirement then EGI would need to seek funding and effort to accomplish this.

4.5.3 Usage of standards

Standards such as ISO 27000 [R 13] and NIST 800-53 [R 15] provide valuable guidance and information in these should be reviewed, even if Resource Centres do not go to the extent of documenting evidence. This may provide them with the opportunity to address weaknesses in their

own practices and procedures. Open standards and checklists may be further examined in the coming months and questionnaires and checklists developed for Resource Centres to the EGI to use to mitigate some security threats. It is probably more efficient to provide EGI specific checklists for sites to use based on standards rather than expect sites to directly use the standards documents.

Questionnaires and checklists based on standards may also be geared towards mitigating any risks that are computed to have a high value in the security risk assessment described in section 6, which are relevant and appropriate for the EGI infrastructure.

Further examination of ISO27000 standards may be considered if sufficient effort is available to work on this to justify the investment in these standards. It is important to carefully consider the advantages and disadvantages of introducing the standards, and the cost and effort verses the benefit. A very selective effort might be more cost efficient.

4.5.4 Consideration of the EGI community

EGI is formed due to the collaboration of various Resource Providers. Most such Resource Providers have limited manpower resources and any requirement or request to them to base their work on standards needs to take this into account. For example, it may be realistic to provide a simple checklist in a similar way to the Swiss Multi Science Computing Grid [R 18] which may help them ensure site security and help people co-ordinating EGI security to ensure that sites participating are carrying out good practices. However, if there were to be a requirement that Resource Centres carry out practices that are too effort intensive to satisfy our security; or to go for formal accreditation, it may mean that some Resource Providers decide to no longer remain part of EGI.

5 OPERATIONAL SECURITY DURING EGI

5.1 Incidents

As of November 2011, EGI CSIRT has handled 12 security incidents, of which 4 incidents affected multiple sites including non-EGI resources. All incidents have been properly resolved in a timely manner. None has caused any major interruption to the production infrastructure.

5.2 Alerts

EGI CSIRT has also issued 14 vulnerability alerts, of which 3 were critical [R 19]. EGI CSIRT assisted all EGI Resource Centres to mitigate these critical vulnerabilities within 7 days.

5.3 Security Service challenge

An information security exercise - the security service challenge 5 was also carried out by EGI CSIRT. This exercise simulated a large scale security incident where in total 40 EGI resource centres participated. The overall feedback has been very positive. A description of this security challenge is available in the autumn 2011 edition of EGI inspired [R 20].

5.4 Pakiti Monitoring

<<Sven Gabriel to add>>

5.5 Security dashboard

A security dashboard has been put into pre-production [R 21]. This allows Resource Centres to conveniently monitor and act on alerts and potential security issues detected by the EGI security monitoring tools. NGI security officers can monitor sites in their NGI and ask sites to correct any errors found. This are input from NAGIOS and Pakiti monitoring.

<<Sven to expand.>>

5.6 Security Training

In order to raise security awareness and improve security of EGI infrastructure, EGI CSIRT also provides security training and security best practices to system administrators. Two security training events were organized at the annual EGI conference. These training sessions have been very well received.

5.7 Software Vulnerabilities

As of December 2011, EGI SVG has handled 47 potential vulnerabilities reported. 30 have been resolved due to either software fixes, operational changes, closed as invalid or duplicates. 17 are either awaiting software fixes or in investigation.

6 PLANS FOR A SECURITY THREAT RISK ASSESSMENT

6.1 Context of this assessment

Security Risk assessment is an on-going activity, and is something that is never complete. It is necessary to re-do and revise security risk assessments from time to time, as the situation is constantly changing, new threats emerge and need to be considered.

6.1.1 Other Grid Security Risk Assessments

In EGEE-III an 'Overall Grid Security Risk Assessment' was carried out. (The report from this was not made public.) This, and lessons learnt from this, form the starting point for the current assessment. Prior to this there was an LCG risk analysis, which is also currently undergoing revision by the WLCG project. Plus there was an OSG risk analysis, which was not made public. The new overall risk assessment by the WLCG project is expected to be completed by February 2012. Since the WLCG infrastructure relies to a large extent on EGI resources, the synergy between the two projects will benefit the risk assessments for either of them, with various security experts contributing to assessments for both.

6.1.2 Scope and level

The ISO27000 definition of a risk is "The potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organisation". Hence we consider the threats to EGI's assets as described in section **Error! Reference source not found.**, from wherever they arise including technical or social threats.

The scope of this may also be considered to be any security threat to or posed by the infrastructure, users of the infrastructure, providers of the infrastructure and information and data stored on the infrastructure. For example, if the production infrastructure were to be used to attack a government organisation, although EGI's computing resources may not be harmed EGI's reputation (which is considered to be an asset) would certainly be harmed especially if appropriate security measures were not in place to mitigate the risk.

The threats are coarse grained; generally they are not specific to a particular technology, although specific technologies may be given as examples to illustrate the threat.

This covers high-level threats, thus allowing the recommendation to management of what actions need to be taken in the overall strategy of risk mitigation, or treatment of threats. It is not generally specific to particular technology, or to a particular case, although cases may be used as examples.

As the EGI expands, both in terms of number of users and number of system administrators, it cannot be assumed that all are trustworthy, and it is necessary to consider 'what if' such a person decided to launch an attack.

This requires a broad participation from a number of people, including security experts in the EGI community.

The actual assessment will be carried out over the coming months, and will not be part of this deliverable.

6.2 Strategy and Methodology for Risk assessment of Threats

6.2.1 Threats

There are various security threats to EGI, from threats that sites are attacked, to threats that confidential data is released, to threats that the infrastructure is used to attack other systems. There are also threats resulting from future changes, and the need to ensure these threats are mitigated as any new methods and technology are introduced.

As many of these threats as possible need to be defined, and the current situation for what is done to mitigate these risks established.

6.2.2 Actuarial computation of risk

The traditional method of computation of risk, e.g. by insurance companies, is the actuarial computation based on statistics. In this case statistics (such as death rates at a given age) are available on which to compute the likelihood and cost of an event. In the case of security threats to EGI we don't have detailed statistics on which to derive a numerical value of the likelihood and impact.

6.2.3 Computation of risk in the absence of statistics

In the absence of statistics from which we can derive a numerical value of the likelihood and impact, an estimate has to be made. In order to produce a numerical value for the risk participants in this assessment will be asked to make a judgement of the likelihood and impact, give a numerical value each of these. These will then be multiplied together to produce a risk.

The Likelihood and Impact will each be a whole number between 1 and 5, and multiplying these together will give the risk. This has been discussed with members of the EGI Security assessment Group and the EGI Security Co-ordination Group and is agreed to be an appropriate strategy. This is the same as that in the EGEE Overall Grid Security Risk Assessment, and it is the strategy being used by WLCG for their risk assessment.

6.2.4 Threat mitigation

In many cases, security threats are mitigated. Systems are in place to minimize the risk of security problems occurring. For example, the checking of sites through the security dashboard as described in section 5.5 detects possible security problems at sites before they are exploited, and the handling of vulnerabilities as in section 5.7 reduces the likelihood of sites being exposed to software vulnerabilities. As well as identifying threats, the team carrying out this assessment will need to establish the current situation, and what mitigation is currently in place.

6.2.5 Inherent and current risk

Two values of the risk are to be computed: the inherent risk, (that is if there were to be no mitigation in place) and the current risk (that with the mitigation in place). This will both demonstrate the steps currently taken to reduce security risk as well as illustrating those activities which currently mitigate risk need to continue, even if the current risk is low.

6.2.6 Suggested further mitigation

Further mitigation may be recommended, especially for threats having a high value for the risk.

6.3 Steps of Risk assessment process

These steps may be carried out in parallel, to some extent. The threats, information on mitigation, will be stored in a spreadsheet.

6.3.1 Establish Team

A team needs to be established to carry out this activity. These people need to be able to spend some time on this, in order to do the work involved. One of the problems with the assessment in [R 1] at the end of EGEE-III was that people who expressed an interest were not able to carry out the assessment. At the time of writing, a group of interested people have already been established. In this case the EGI Security Assessment Group is being formed which consists of security experts from various NGIs and security groups in EGI and other Grid projects.

6.3.2 Select Threats and assets

Here a comprehensive list of threats and assets is produced. This is done considering the following:

- Listing the assets in detail as described in section **Error! Reference source not found.**.
- Listing every threat that members of the team can think of.
- Examining other checklists produced e.g. by SANS institute.
- Looking at other work, such as WLCG's list of threats if it is available.

The threats, where possible, should be general and coarse grained rather than low level or software specific. With the selection of the threat it should be clear what asset or assets are under threat.

6.3.3 Select a 'Contact' for each threat

Each threat should have a 'contact', the person who makes it their business to know what is happening regarding that threat and keeps information up to date. The 'contact' is the most likely person to suggest mitigation for threats computed as having a high risk. If possible, this will be someone who is already working in this area.

Note that the 'Contact' is not responsible if the threat is carried out.

The 'Contact' may not necessarily be a member of the team carrying out the Risk assessment, but is someone prepared to provide information relevant to the threat.

6.3.4 Establish Current situation

The contact for each threat should establish the current situation, and what mitigating steps are in place.

6.3.5 Computation of Risk

The risk is computed. It is preferred that a consensus is reached. However, it may be that each member of the team provides their view on the value, and the average taken.

Risk is computed both for the inherent risk, and for the current situation with the current mitigation in place.

It would be desirable to get the team around a table for a couple of days to discuss and see if they can come to a consensus on the Risks.

6.3.6 Suggest Mitigation

Where possible, the team carrying out the assessment along with the 'Contact' of the risks suggests mitigating action, or treatment of the risks, especially if insufficient mitigation is currently in place.

6.3.7 Complete and present to management

After the assessment is complete the findings are presented to management, including description of possible treatment or mitigation of risks.

6.4 Effort and schedule

6.4.1 Estimate of effort needed

It is difficult to accurately estimate the effort needed, especially as we have not yet established whether we will go for a larger number of threats (similar to the security Risk assessment that was carried out during EGEE) or a very small number of high level threats (similar to that carried out by WLCG). Here we attempt to make a guess at the upper and lower level of effort involved.

For an upper estimate assume that 12 members of the Security Assessment group each spend 2 day on threat selection, and each spend 2 days assessing the threats that is 48 person days. If we assume 1 person day (on average) is spent per threat checking the situation and writing the mitigating action, then assuming 50 threats then is about 50 days. Allowing for co-ordination and the writing up reports the total effort required is of the order of 100 to 120 person days. Some members of the project think that is an appropriate estimate, and does not seem to be overestimated considering the scale and complexity of EGI.

The WLCG Computer Security Risks analysis (which is still a work in progress) considers a small number of very high level threats, of the order of 15. We can base a lower limit of the time needed on this. If we assume that we carry out a similar selection, and spend just 0.5 days per person on threat selection, and 1 day per person assessing the risk, this gives 18 days. Plus 1 day per threat on the establishment of the situation and mitigation, this gives 33 person days. With the writing of the report this is 35-40 person days.

A mid range estimate is if we select 30 threats. If the group again spends on average 2 days per person between threat selection and risk assessment, which is 24 days. If it is then assumed that around 1 day is spent per threat, on establishing the situation and mitigation that is 30 days. This would mean we would be asking for the participants to spend of the order of 4 days of effort in total on this task. In addition, an extra 5-10 days would be needed from the co-ordinator, to organise the work and write the report. In this mid-point case the order of a total 60 person days may be needed.

6.4.2 Plans for Schedule

Here is a table with a suggested schedule. As can be seen from above in section 6.4.1, it's hard to estimate the amount of work involved so the schedule is very preliminary.

Task	Carried out by	Notes
Selection of Threats and assets under threat.	End January 2012	Should be done by e-mail. This includes 'Contact' for each threat. (see 7.3.5)
Establishment of current situation and current mitigation in place	Mid February 2012	Again by e-mail
Risk Assessment	End February 2012	Would be good if this could be done round a room, i.e. a 1-2 days meeting. If not, by e-mail and maybe some EVO discussions
Suggest any further mitigation, and write report	Mid March 2012	Suggestions for mitigation and report writing by co-ordinator can be done in parallel.

6.4.3 Frequency of re-assessment

Security risk assessment is an on-going activity, something that is never complete. It is necessary to re-do and revise risk assessments from time to time, as the situation is constantly changing and new threats emerge. It is recommended that as well as carrying out a Risk Assessment in early 2012 the assessment is repeated around 18 months later, towards the end of 2013. This will allow progress during this time to be gauged and enable any remaining High risks to be addressed before the end of the EGI-InSPIRE project.

7 THREATS

This section does not attempt to list all threats, but attempts to give some idea of the approach to selecting threats and describe what types of area are included. The team carrying out the assessment will define the list. A draft list with some comments and information has already been produced, and this will be refined by those carrying out the assessment.

7.1 Where are the Threats from and what assets are under threat?

Threats may come from many sources; the primary ones are external attackers, legitimate users, and service providers (including site administrators). Threats may also come from technical (hardware or software) failure.

Threats may be to the infrastructure, whether physical damage or cyber attack. Threats may be to privacy of data or information, to the service provider (in that the service provider may suffer if the site is used for unlawful activities.) Also, security attacks may affect users due to loss of service. Threats may also be to the reputation of EGI.

To list every possible problem that may occur and every source of attack would involve a very long list. The approach is mainly to list the main threats to the identified assets, such as users, data, infrastructure, external sources, and the reputation of EGI. Some areas, where appropriate, primarily the source of threats is listed. If an action can be carried out by a user, it can also be carried out by an attacker who gains access to the system. Prevention lies in both preventing access to attackers, as well as monitoring usage for general miss-use.

All threats are 'high level' threats. Details may exist in other documents which may be referred to.

7.2 Responsibility and scope

As well as considering the threat and the asset under threat, the plan is also to consider who is responsible for ensuring the threats are mitigated. This may be the EGI-InSPIRE project, the Resource Provider (RP), or someone else. For example, physical security at sites is the responsibility of individual resource providers.

7.3 Properties of a threat

7.3.1 Title

This is a sentence defining the threat.

7.3.2 Category

The category of the threat, categories may include for example physical threats, technical threats.

7.3.3 Identifier

This is a simply identifier for the threat, including category and a number.

7.3.4 Asset

This is EGI asset or assets which are at risk from this threat.

7.3.5 Contact

The expert or person whose duty it is to find out details of the current situation, mitigation in place.

7.3.6 Responsible

The 'responsible' is person or persons responsible for carrying out any mitigating action. This may be to reduce the likelihood of the threat being carried out, or the impact if it is carried out. This applies equally to mitigation currently in place to proposed mitigation resulting from this assessment.

7.3.7 Description

This is a description of the threat; it includes an explanation of the potential impact on the asset or assets under threat.

7.3.8 Inherent Risk

This is considered as the product of the likelihood and impact. This is the risk if there were to be no mitigation in place.

7.3.9 Current Mitigation

This is a description of the Mitigation currently in place to reduce the likelihood of the threat being carried out or its impact.

7.3.10 Current Risk

This is again the product of the likelihood and impact. This is the risk with the current mitigation in place.

7.3.11 Notes and recommendations

This includes any recommended treatment or further mitigation of the risk, to reduce either the likelihood of the threat being carried out or the impact.

8 FUTURE WORK

This document presents the strategy and the plan for the security risk assessment of the EGI infrastructure. The actual risk assessment will be implemented in the first quarter of 2012, and its release is expected by the end of March as explained in the schedule reported in the section **Error! Reference source not found.**. There are also plans to repeat the risk assessment18 months after the first version, towards the end of 2013.

9 REFERENCES

R 1	The EGI InSPIRE Description of Work (DoW) https://documents.egi.eu/secure/ShowDocument?docid=10
R 2	The International Grid Trust Federation (IGTF) http://www.igtf.net/
R 3	MyProxy http://grid.ncsa.illinois.edu/myproxy/
R 4	SPG wiki https://wiki.egi.eu/wiki/SPG
R 5	SVG description http://www.egi.eu/policy/groups/Software_Vulnerability_Group_SVG.html
R 6	SVG wiki https://wiki.egi.eu/wiki/SVG
R 7	CSIRT description http://www.egi.eu/policy/groups/EGI_Computer_Security_Incident_Response_Team_EGI_CSIRT.html
R 8	CSIRT wiki https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
R 9	EU Grid PMA website http://www.eugridpma.org/
R 10	EMI http://www.eu-emi.eu/home
R 11	Initiative for Globus in Europe http://www.ige-project.eu
R 12	The international Standards organisation (ISO) http://www/iso.org/
R 13	ISO 27000 series of standards http://www.27000.org/standards.htm
R 14	The National Institute of Standards Technology (NIST) http://www.nist.gov/index.html
R 15	NIST SP 500 53 Information security http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
R 16	NIST FIPS 199 Standards for Security Categorization of Federal Information and Information systems http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
R 17	NIST FIPS 200 Minimum Security Requirements for Federal Information and information systems http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
R 18	Swiss Multi-Science Computing Grid (SMSCG) - information for site administrators http://www.smscg.ch/www/admin/
R 19	Operational security alerts https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts
R 20	Description of 2011 Security Service Challenge http://www.egi.eu/results/newsletters/Inspired_Autumn_2011/Report_on_the_SSC5.html
R 21	Security operations dashboard https://operations-portal.egi.eu/csiDashboard.




e-infrastructure