EGI-InSPIRE

SECURITY RISK ASSESSMENT OF THE EGI INFRASTRUCTURE

EU DELIVERABLE: D4.4

Document identifier:	EGI-SCG-D44-863-v0.6
Date:	**15/11/2011**
Activity:	**SA1**
Lead Partner:	**EGI.eu**
Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC?**
Document Link:	https://documents.egi.eu/document/863

Abstract

This document Reviews Security in the EGI infrastructure. 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 few months is described.



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	<<The lead author/editor>>		
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
1			

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/.

<<The authors should check if the acronyms are covered by the glossary page and if the definition is still correct; all the amendments should be communicated to glossary@egi.eu>>

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

<< The text should provide a summary of the full report so that the reader can 'in a page' understand the problem it has been written to cover. This includes an overview of the background material and motivation for the report, a summary of the analysis, and the report's main conclusions.>>

<<Linda to write after most other sections complete>>



TABLE OF CONTENTS

1 INTRODUCTION

1.1 From the EGI DoW

In the DoW 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 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 attempts to answer 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 applicable to the Grid infrastructure.
- A description 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 attempt to answer the question, "what does it mean to be secure on the grid?", and "what assurances can we give to users, resource providers and others?"

2.1 Aims of EGI and EGI security

The EGI home 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 on the EGI 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 EGI Infrastructure. Traditional approaches to security may not be appropriate in the EGI environment. Many of the traditional approaches used by many commercial companies are largely aimed at preventing widespread access yet within the EGI environment a wide user base is encouraged to access the resources. Some aspects of a traditional approach to security are appropriate, such as many aspects of good practise in management of resources. The resources which constitute the EGI Infrastructure are managed by the various Resource Providers (RPs).

2.2 What should users expect?

The system needs to be suitable for use: users need convenient access to the resources and be confident that the Data and Information Security is appropriate. They also need to be confident that they cannot accidently damage the system, be liable for unintentional actions that caused serious problems or for actions for which they are not responsible. If charges are implemented for use of resources, users need to be confident that neither they nor their institute can find themselves with a big bill they did not expect.

2.3 What should Resource Providers expect?

Resource Providers need to be confident that the mechanisms and technology enabling the Grid do not lead to insecure sites, do not lead to damage to their sites, access beyond intended rights such as to other resources on the sites, or damage their reputation. Resource Providers also need to be confident that they receive appropriate support in the secure deployment of the Grid technology, and that they are not going to find themselves legally liable for actions carried out by others, such as unlawful use of copyright software or other illegal activities.

2.4 Data and Information Security

2.4.1 Financial Data

The EGI infrastructure does not store or process any Financial information or data. The security systems are not designed to deal with financial data, such as credit card details. The IGTF identity system on which security is based also does not provide for authentication for use of such data.
<David Groep may expand/correct>

2.4.2 Personal identity and accounting data

Delegated proxies are stored widely in the infrastructure, and are generally accessible to system administrators. This means that we have to trust system administrators not to impersonate users.

Long lived proxies are stored in the MyProxy server, which has carefully controlled access, and facilities the renewal of proxies used for long lived jobs.

Accounting data is also stored on the Grid (clarify where/how)

<<Maarten Litmaath to improve>>

2.4.3 General Scientific data

Scientific data is generally stored in an unencrypted form, but readable only by those authorized. Site administrators can generally access all data stored on the services for which they are responsible. Users need to be sure that their data is stored reliably, and available for access. This means appropriate procedures need to be in place, for example backing up data and/or storing in more than one place.

2.4.4 Other Scientific Data

If certain applications, e.g. biomedical, need to keep their data confidential it is their responsibility to store the data in encrypted form and manage the encryption keys. For encrypted data, site administrators should not be able to access both the data and the keys.

2.5 EGI's Role

EGI's role is to collaborate with NGIs, Resource Providers and Virtual Research communities to ensure that the Infrastructure is as secure as possible. To tackle this complex problem space EGI 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.

2.5.1 EGI's responsibility

EGI's responsibility includes collaborating with NGIs, Resource Providers, Users, and Virtual Research Communities, to ensure appropriate controls are in place, and ensure that the procedures available ensure the smooth and secure running of the Grid. This includes ensuring that the technology which enables the sharing of resources in the EGI infrastructure is as secure as possible. In particular, it includes ensuring that software distributed by EGI or recommended by EGI for installation by Resource Providers is as secure as possible.

EGI should also encourage Resource Providers, Users, and others who interact with the Grid to carry out good practices.

<<should there be more of this? Dave Kelsey add/comment?>>

2.5.2 EGI's responsibility is finite

The EGI Infrastructure is not a single domain and it is not possible to have complete control over all resources.

For example, the secure operations of the various Resource Providers that make up the infrastructure cannot be EGI's responsibility, but the responsibility of the various sites, even though the secure running of sites is important to the secure running of the overall EGI infrastructure. Sites are responsible for incident handling, while EGI does provide an incident handling procedure which Resource Providers are expected to follow and members of the CSIRT Team are often able to help, EGI has limited access to log files, and Resource Providers will need to do most of the work themselves in the case of an incident.

EGI cannot ever guarantee security, but should do all it can to mitigate risks, help Resource Providers mitigate risks, or encourage others to mitigate risks from identified threats.

<<should there be more of this? Dave Kelsey add/comment?>>

2.6 The EGI Ecosystem

<<Describe ecosystem from services provided by RPs and NGIs, to EGI.eu training, web pages, users, etc. High level, no detailed >>

<<Linda to draft, others to add/comment on later>>

2.7 EGI's Assets

Security can be seen as protecting assets. Some of EGI's assets are intangible, such as EGI's reputation.

<<Linda to draft, others to add/comment later>>

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 one another and is implicit to the management of risk to EGI's assets. Each group carries out activities which are designed to make the Grid secure, and is important in the management of risk.

(Should the links be proper references, or are they better as just links?)

<<Dave Kelsey to expand/improve>>

3.1 The EGI Security Policy Group

The **Security Policy Group (SPG)** is responsible for developing the policy needed to provide NGIs with a secure, trustworthy distributed computing infrastructure. The SPG output defines the behaviour expected from NGIs, Resource Providers, Users and other participants to maintain a beneficial and effective working environment.

More information is available from the SPG Wiki page at https://wiki.egi.eu/wiki/SPG

Various approved procedures carried out by other security groups implement the various policies.

<<Dave Kelsey to expand/improve/check>>

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.

More information is available at

http://www.egi.eu/policy/groups/Software_Vulnerability_Group_SVG.html and from the SVG Wiki page at https://wiki.egi.eu/wiki/SVG

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 ensures 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.

<<Mingchao Ma to expand/improve/check>>

More information is available at

http://www.egi.eu/policy/groups/EGI_Computer_Security_Incident_Response_Team_EGI_CSIRT.html and the EGI CSIRT public wiki at https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

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 ensure that there is coordination between the operational security, the security policy governing the use of the production infrastructure and the technology providers whose software is used within the production infrastructure. Membership consists of the chairs of the SPG, SVG, CSIRT, representatives from the EUGridPMA, EMI and IGE security Team (i.e. software providers), and the EGI Operations manager and EGI director.

3.5 Related Groups

3.5.1 The EU Grid PMA

The EUGridPMA is the international organisation to coordinate the trust fabric for e-Science authentication in Europe. The various country certificate authorities (who issue certificates to users and resources) are members of the EUGridPMA, and certificates issued by such authorities are accepted as identification in the EGI Infrastructure. More information is available at the EUGridPMA website at http://www.eugridpma.org/

<<David Groep to improve/expand/check>>

3.5.2 Software Security in EMI

Much of the middleware deployed in the EGI Infrastructure 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 at http://www.eu-emi.eu/home

<<John White to improve/expand/check>>

3.5.3 Software Security in IGE

Some sites in the EGI infrastructure use middleware produced by Globus. Similar security functionality for the sharing of resources on a large scale is available in IGE. For more information on IGE http://www.ige-project.eu/

<<Oscar Koeroo to improve/expand/check>>

3.6 Diagram of relationships between groups.

<<Linda to draw and add>>

4 PRACTICES AND STANDARDS

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

4.1 Standards for information management

4.1.1 ISO standards

The International Standards Organisation (ISO) [R 2] develops standards in various areas. The ISO 27000 series [R 3] of standards concern information technology, security techniques and information security management systems. The 3 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.

ISO standards need to be purchased, they are not available free of charge and the cost is not trivial. A full set of 27000 series standards based on 1 user would be at least 500 Euros, and it is not clear whether an EGI licence could be purchased or what cost it would be. Various people within EGI have their own copy, or sight of a copy in their institute.

4.1.2 NIST Standards

In the US the National Institute of Standards and Technology (NIST) [R 4] is an agency of the US department of commerce. The NIST publication SP 800-53 is entitled 'Information Security' [R 5]. 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 6] 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 7] 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 Grid and a Security Questionnaire for Infrastructure providers was produced based on this standard. This is available from the Swiss Multi Science Computing Grid information for site administrators. [R 8] 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 funded by the DoE were obliged to have their systems audited according to NIST standards. Even though their systems fell into the lowest category according to the DoE standard FIPS199 [R 6] 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 the OSG carried out a mapping of the NIST SP800-53 to the Grid in 2007, however this is not available publicly.

<<David Groep to check >>

4.2.3 EGI Procedures partially based on standards

Some of the EGI operational procedures are partially based on standards, such as the incident handling procedure...
<<Giuseppe Misurelli to write >>

4.3 Technological standards

Basing the EGI security infrastructure on technological standards helps in ensuring interoperability between non-uniform infrastructures and reduces 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.

<<John White to modify and complete >>

4.4 Application of technological Standards in the EGI community

4.4.1 EGI UMD middleware based on standards

<< John White to complete - 2-3 examples >>

4.4.2 Other examples of technology based on standards

<< Riccardo Brunetti to complete – 2 examples probably enough >>

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

4.5.1 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.

4.5.2 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 openly available for use. Some checks are appropriate on a per site basis, some may be appropriate in a wider EGI context.

4.5.3 Detailed examination of ISO27000 standards

The appropriate ISO27000 standards are being examined by WLCG during the coming months. These may further be examined in detail including their relevance to EGI. This may include the production of checklists and/or questionnaires for Resource providers, to ensure that they maintain security.

<<Maarten to correct/add as appropriate?>>

4.5.4 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 our input.

4.6 Conclusions on standards and EGI

4.6.1 Practices in EGI

Resource Providers are generally experienced in managing systems, and sites are likely to be mostly well managed. Resource providers tend to have good practices in place, whether or not they are formally based on standards. EGI policies and procedures are followed by resource providers to ensure that sites are sufficiently secure, and 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 EGI infrastructure.

4.6.2 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.

4.6.3 Usage of standards

Standards such as ISO 27000 and NIST 800-53 provide valuable guidance for sites, and information in these should be looked at in details even if Resource Providers 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. To directly use these standards on a per site basis is very time consuming, as they are lengthy and not easy to use. Open standards and checklists may be further examined in the coming

months and questionnaires and checklists developed for Resource Providers to the EGI to use to mitigate some security threats.

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.

4.6.4 Consideration of the EGI community

The EGI infrastructure 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 8] 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 sites carry out practices that are too effort intensive to satisfy our security, or for sites to go for formal accreditation it may mean that some sites decide to no longer remain part of the EGI infrastructure.

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 EGI infrastructure.

5.2 Alerts

EGI CSIRT has also issued 14 vulnerability alerts, of which 3 were critical (https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts). 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.

5.4 Security dashboard

A security dashboard has been put into pre-production. https://operations-portal.egi.eu/csiDashboard.

This allows Resource Centres to conveniently monitor and act on alerts and potential security issues detected by the EGI security monitoring tools.

6 PLANS FOR A SECURITY THREAT RISK ASSESSMENT

6.1 Context of this assessment

6.1.1 Other Grid Security Risk Assessments

In EGEE-III an 'Overall Grid Security Risk Assessment' was carried out. [R 1] This, and lessons learnt from this, forms the starting point for this 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 (this was not made public).

<<Maarten Litmaath to improve/ include something on the current WLCG one>>

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 2.7, 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 EGI infrastructure, users of the infrastructure, providers of the infrastructure and information and data stored on the infrastructure. For example, if the EGI 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 Grid 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 Risk assessment of Threats

6.2.1 Threats

There are various security threats to the EGI infrastructure, from threats that sites are hacked, 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 the EGI infrastructure 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.

TBD - between 0 and 1 for likelihood. Between 1 and 100 for impact?

Then this gives between 0 and 100. 25 or more warrants action? Or see what happens?

6.2.4 Threat mitigation

In many cases, security threats are mitigated. Systems are in place to minimize the risk of security problems occurring. 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.

6.3.2 Select Threats

Agree on the threats and the level of detail of the threats. 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 an '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 present finding to management, this includes possible treatment or mitigation of risks.

7 THREATS AND CATEGORIES

This section does not cover all possible threats, but is intended to describe what types of area are included. The first draft of the threats is in the spreadsheet accompanying this document <<deleted from document server. Needs revision, and stuff in there that shouldn't be public>>. However, the team carrying out the assessment may refine this list. This list may also be refined on future updates of the assessment process.

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 infrastructure, users, data and 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 Categories of threats

<<Linda to revise probably less detail. >>

Some possible Categories of threats are:

- Software Vulnerabilities
- Operational and Configuration Vulnerabilities
- General Technical Threats to the infrastructure
- Physical Security Threats to infrastructure
- Threats arising from Security Incidents
- Threats to external parties
- Data security and Integrity
- Software Security and Integrity
- Confidentiality
- Illegal and general miss-use of resources
- Threats from users
- Threats to users
- Threats from trusted staff (site administrators, CA and VO administrators)
- Threats to trusted staff and service providers.
- Threats arising from Security services (e.g. CA and VO management)

- Threats from management decisions
- Security Threats arising from social engineering
- Threats from move to virtualization
- General threats from installation of new software and technology.

7.3 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 project, the site, or whoever else.

E.g. Physical security at sites is the sites responsibility. Ensuring UMD software does not contain vulnerabilities or malware is EGI DMSU responsibility.

7.4 Some examples of threats

<<Linda to complete>>

7.4.1 Resources used for on-line attack to 3rd party

(Threats to 3rd party)

If the Grid were to be used to attack a 3rd party, EGI and those who deploy Grids could be considered liable, especially if suitable measures have not been taken to minimize the Risk. It could easily lead to pressure to immediately stop deploying the Grid infrastructure and thus deny all use of the Grid for a considerable time until sufficient measures are in place. Such attacks could include DoS, or attempts to crack a password by attempting to log on from large numbers of WNs across the grid.

7.4.2 Confidential information leaked due to system compromise

(Confidentiality.)

7.4.3 Trusted staff attack system after leaving

(Threats from trusted staff)

8 REFERENCES

R 1	The EGEE Overall Security Risk Assessment https://edms.cern.ch/document/1039446/1 (note this is not public)
R 2	The international Standards organisation (ISO) http://www/iso.org/
R 3	ISO 27000 series of standards http://www.27000.org/standards.htm
R 4	The National Institute of Standards Technology (NIST) http://www.nist.gov/index.html
R 5	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 6	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 7	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 8	Swiss multi Science Computing Grid information for site administrators http://www.smscg.ch/www/admin/