EGI-Engage

The evolution in security policies, procedures and best practices in EGI

D5.3

Date	24 April 2017
Activity	WP5
Lead Partner	STFC
Document Status	Final
Document Link	https://documents.egi.eu/document/3027

Abstract

This deliverable report describes the work done by EGI-Engage SA1/WP5 to evolve the EGI security operations, policies, procedures and best practices. This aims to mitigate the security risks introduced to the EGI Infrastructure as a result of its new services, technology, trust models, and usage scenarios. The work has been split into 5 different sub-tasks and these are reported on in turn: security requirements and risk assessment; the evolution of operational security procedures, including forensics; the development of a new trust framework and new security policies; an updated security challenge framework; and updating of the software vulnerability handling process. Plans for the remaining 6 months of the project, for exploitation and for dissemination are also presented.

This material by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License.

The EGI-Engage project is co-funded by the European Union (EU) Horizon 2020 program under Grant number 654142 http://go.egi.eu/eng

COPYRIGHT NOTICE

This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EGI-Engage project is co-funded by the European Union Horizon 2020 programme under grant number 654142.

DELIVERY SLIP

	Name	***Partner/Activity***	***Date***
From:	V. Brillault L. Cornwall S. Gabriel D. Groep D. Kelsey	CERN/WP5 STFC/WP5 Nikhef/WP5 Nikhef/WP5 STFC/WP5	2017-04-12
Moderated by:	M. Krakowian	EGI Foundation	
Reviewed by	V. Ciaschini I. Collier E. Fernández T. Ferrari (AMB and PMB)	INFN STFC EGI Foundation EGI Foundation	2017-04-19
Approved by:	AMB and PMB		2017-05-03

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V0.1	2017-03-09	Document creation	D.Kelsey/STFC
V0.2	2017-04-12	Draft submitted to reviewers	D.Kelsey/STFC
V0.3	2017-04-20	Draft responding to all reviewers' comments	D.Kelsey/STFC
V0.4	2017-04-23	Draft in correct template, with abstract, executive summary and plan for exploitation and dissemination	D.Kelsey/STFC
Final	2017-05-03	Final version	D.Kelsey/STFC

TERMINOLOGY

A complete project glossary and acronyms are provided at the following pages:

- https://wiki.egi.eu/wiki/Glossary
- https://wiki.egi.eu/wiki/Acronyms

Contents

Executive summary

The EGI-Engage task SA1.2 (WP5) is charged with developing security operations, including policies, procedures and best practices, to meet the requirements of new trust models, new developments and new usage scenarios as these evolve in EGI-Engage.

EGI needs to protect its assets and keep its services secure and available. This involves the standard balance between security, confidentiality and integrity with availability and ease of use. To achieve all this, we use the usual ongoing cyclic process based on threat analysis, security risk assessment, mitigations and controls. In EGI-Engage task SA1.2 we have considered in particular the evolution of the deployed services and technology, new trust models, and new usage scenarios.

The work was split into 5 different sub-tasks:

- ***Security requirements and risk assessment for new services, technology, and deployments***
- ***The evolution of operational security procedures, including forensics***
- ***Develop a new trust framework and develop new policies***
- ***Develop the security challenge framework***
- ***Develop the software vulnerability handling process to adapt to new technology and deployments***

This document reports progress made in each of these sub-tasks in turn and then presents our plans for the final six months of the project and also for exploitation and dissemination.

A new security threat risk assessment was performed, focusing in particular on the security of the EGI Federated Cloud service (FedCloud). We identified that 24 out of the 103 risk values, calculated as "likelihood" multiplied by "impact", were high enough to warrant further work on mitigation. Early on, it was agreed that an important security risk mitigation in the EGI FedCloud was to require the use of endorsed/approved Virtual Machine (VM) images or Virtual Appliances. Another area of concern was the difficulty of detection and handling of security incidents in the EGI FedCloud as were threats arising from vulnerabilities and their handling.

Many developments have been made to the EGI CSIRT/IRTF procedures. These included the *EGI Security Incident Handling Procedure* and forensic guidelines. We have improved the *EGI-CSIRT Critical Vulnerability Handling procedure*, to be more readable and accessible and to address issues related to the new concept of Virtual Appliances. IRTF developed internal tools in order to decrease the number of repetitive tasks and to standardise the different messages sent.

Plans for an enhanced security challenge framework for the EGI FedCloud were agreed by the EGI CSIRT. The framework has been developed and has been tested at a number of sites. More work, however, is required in the usage of contextualisation and configuration of EGI FedCloud sites before a full challenge can be run.

New security policies have been produced and others have been revised and updated during the EGI-Engage project. The changes made were to address the evolution of EGI services and technology and to mitigate risks identified in the new security risk analysis. This included a major revision to the top-level security policy document; an updated version of the "Acceptable Use Policy", generalised to include all EGI service offerings; a new policy and guidelines document entitled "The EGI Science Applications on-demand Security Policy", produced in collaboration with SA1.3; a complete revision of the policy on Data Protection to turn this into a more general framework to be used by all services. Other policy work included a new policy on Acceptable Authentication Assurance and updating of the terminology used by all remaining old security policies that needed no other updates.

We have continued to play a leading role in the Interoperable Global Trust Federation (IGTF) through leadership of the EUGridPMA. We have led the development of new trust and policy related to AAI and federated identity, with the aim both of making the appropriate levels of assurance available to research infrastructures and to lower the barriers of entry. This work is a collaborative activity with EGI-Engage JRA1, with AARC (EU H2020) and the REFEDS community.

The scope and range of the IGTF trust anchors has been evolved, to make use of new assurance levels, in particular the 'identifier-only' trust assurance level ("DOGWOOD") that provides persistent non-reassigned identifiers to entities. This allows the distribution of authentication responsibilities between identity providers, research communities, and resource centres, and this has been piloted with structured user communities (WLCG and ELIXIR), together with the integration of the *RCauth.eu* AARC pilot service and also with the new EGI AAI Access platform.

The EGI Software Vulnerability Group carried out a major revision of the Software Vulnerability Issue handling procedure to address the evolving EGI services. For example, when a critical vulnerability is found relating to a Virtual Appliance, this needs to be updated urgently by those responsible for the VA.

In the WISE community[1], through its representation in the steering committee and leadership of working group activities, EGI benefits from better alignment of security practices and increased input into its risk assessment, training and trust programmes. EGI leads the SCIV2 working group, where work is ongoing on a new version of the SCI trust framework. The construction of comparative policy frameworks allows easy movement of researchers and data across multiple Infrastructures, whilst the construction of the human network through periodic WISE workshops has also established communication channels for operational security activities.

Plans for the remaining 6 months of EGI-Engage have been made and include more risk mitigation, updated user and research community security policies, updated procedures for the CSIRT and IRTF, performing the new Security Service Challenge, and more updates to SVG. Our plans for exploitation and dissemination are also reported.

[1] https://wise-community.org/about-wise/

1 Introduction

The EGI-Engage task SA1.2 in Work Package 5 is charged with developing security operations, including policies, procedures and best practices, to meet the requirements of new trust models, new developments and new usage scenarios as these evolve in EGI-Engage.

This Deliverable (D5.3) report describes the achievements and outputs of the activity and the work that has been done to date in EGI-Engage WP5 task SA1.2 (Development of Security Operations). It also presents the plans for SA1.2 during the final 6 months of the project.

It is well established best practice, e.g. as described in the ISO 27000 series of standards, that information security is best tackled as an ongoing process involving regular security risk assessment, deployment of new/updated mitigations and controls (technical, operational and policy), followed by operational deployment, monitoring and review, then back to the updating of the risk assessments etc. This is what used to be known as the "Plan-Do-Check-Act" cycle. The work of SA1.2 (Development of Security Operations) has been following this approach in evolving the EGI security policies, procedures and best practices in response to the new technology and services being developed and deployed on the EGI infrastructure and to the ever-changing landscape of security threats.

The SA1 funding for this work, spread across 5 individual people integrates to less than 1 full time person, so to make good progress on so many different aspects of operational security we have had to collaborate with other effort and/or individuals funded by both the EGI Core services funding and also by various sources of institute and national funding.

Some of the highest security risks have been identified as arising from the new and evolving EGI Cloud Compute service[2], hereafter referred to as the "EGI FedCloud". It is important to stress that much of the effort involved in these SA1.2 activities has been spent by attending many meetings of the EGI FedCloud group, presenting the security teams concerns and proposals and by encouraging the Cloud Compute providers to understand the importance of information security. We have persuaded them gradually to accept the need for the adoption of new procedures and technical controls. Much of the success here resulted from the detailed analysis of security incidents that took place on the EGI FedCloud and jointly agreeing the lessons learned and the changes that were/are required.

The best way of presenting our aspirations for the work in this task is to remind the reader of the project proposal. From the Technical Annex of EGI-Engage, the work of WP5 task SA1.2 (Development of Security Operations) was described as follows:

[2] https://www.egi.eu/services/cloud-compute/

This task will develop security operations, including policies, procedures and best practices, to meet the requirements of new trust models, new developments and new usage scenarios as these evolve in EGI-Engage. The work is split into the following activities:

1. ***Security requirements and risk assessment for new services, technology, and deployments.*** *The new developments and evolving usage scenarios in EGI-Engage will involve trust models different from the core infrastructure used in EGI-InSPIRE. The task will ensure that the security requirements and the trust model are defined. Any security problems will be addressed and risk assessment associated with new deployments will be developed, to drive operational security in the evolved environment, to keep services secure and available and to mitigate the serious risks.*

For a report on the activities in this sub-task, please see section 2 of this document.

2. ***The evolution of operational security procedures, including forensics.*** *Refine and extend the current security procedures and tools for incident response and forensics, for example: to take into account new kinds of players (e.g. cloud resource providers), or to extend the emergency suspension mechanism to cover new kinds of services. The security procedures related to other EGI operational procedures will also be modified as required.*

See section 3.

3. ***Develop a new trust framework and develop new policies.*** *In collaboration with other infrastructures, we will define new additions to a new policy framework to handle the new deployment and usage scenarios as they evolve in EGI-Engage. In collaboration with JRA1.1 the task will validate the architecture assumptions through testing in partnership with user communities under realistic production conditions and provide support on AAI security issues in close coordination with the EGI CSIRT and SVG. The task will provide recommendations on how best to sustain this important activity beyond the end of EGI-Engage.*

See sections 4, 5, and 7.

4. ***Develop the security challenge framework.*** *Experience from EGI-InSPIRE has shown that performing security service challenges on the operational infrastructure is useful confirm that there is sufficient audit information for traceability of any incident, that procedures and tools are sufficient and that participants are trained and aware of the need to participate in incident response. The framework for these security challenges will be modified and extended to meet the evolving scenarios.*

See section 3.5.

5. ***Develop the software vulnerability handling process to adapt to new technology and deployments.*** *Software vulnerability issues in the EGI core infrastructure have been handled*

through a close relationship with the technology providers, many of whom supply members of the Software Vulnerability Group (SVG). The general principles will remain, including the assessment of risks and the issuing of advisories. In the evolving scenarios of EGI-Engage there are, however, likely to be different types of relationship with the technology providers, especially when this does not involve membership of SVG. The procedures and methods for handling vulnerabilities in EGI-Engage will evolve accordingly.

See section 6.

This document now presents the work performed in each of these areas and the resulting evolved procedures, policies and best practices in operational security. There are some areas where more work is still required. This is planned for the final 6 months of the project and presented in section 8. We also present our plans for exploitation and dissemination in section 9.

2 Security requirements, threat risk assessment and mitigations

An important aim of the security activity in EGI is to reduce or mitigate the risk arising from the many security threats to the Infrastructure. In order to understand the threats, and which pose the highest risk, a security risk assessment needs to be regularly performed. A security threat risk assessment was carried out towards the end of 2015, and completed during the early 2016, focusing on security in the EGI FedCloud. The methodology was similar to a risk assessment carried out in 2012, where the focus was on other Compute services, primarily HTC Compute[3] at the time. More details of the risk assessment methodology used are in section 6 of Deliverable D4.4 from the EGI-InSPIRE project (https://documents.egi.eu/document/863).

Firstly, a risk assessment team was established. A draft list of threat categories and threats within each category was then written. A member of the team was assigned to each category, whose job it was to improve the list of threats and establish the current situation including the mitigations in place. Each member of the team could additionally comment on any other threats they wished. When the list was agreed, each member was asked to rate each threat in terms of 'Likelihood' and 'Impact', both between 1 and 5, according to a set of guidelines. The risk value, the product of the Likelihood and Impact, a number in the range 1 to 25, was computed for each individual threat. These individual ratings of risk were then averaged over the team members and the standard deviations were also recorded as a measure of the spread of the ratings. Some of the risks were then discussed, particularly those with a high-risk value or where there was a high standard deviation on the risk assessments. Any member could request to discuss any threat they wished. A report was written, including work in progress to mitigate some of the threats with highest risk value, and to recommend mitigation for some others. Further work is planned for

[3] https://www.egi.eu/services/high-throughput-compute/

mitigation of other threats. Producing suitable mitigations takes time and effort and as such is an ongoing activity. Please note that this report is not a public document.

The work was carried out by e-mail and by video conferences. A spreadsheet was developed containing 103 threats identified in 19 categories. Ten members of the team estimated the Likelihood and Impact for the various threats. In the assessment performed in 2012, 18 threats out of 75 in total were reported as having a risk value of 8 or more, whereas in this assessment we find 24 out of 103 have a value of 10 or more, and almost half have a value of 8 or more. Hence it appears that the team considers the likelihood and/or impact of problems to be greater than 3 years ago. This may be explained that people feel there is genuinely more risk with the EGI FedCloud, that there is less control over what technology is used on the Infrastructure, that more new technology is being used, or it is being operated in a less secure way, or that the general threat landscape is greater. We should also note however that as only 4 people were also members of the 2012 team last time the differences may be down to different normalisations and new people estimating things differently.

It was agreed that an important security risk mitigation in the EGI FedCloud was to require the use of endorsed/approved Virtual Machine (VM) images or Virtual Appliances, i.e. VMs that have been created and endorsed by Virtual Organisation managers rather than allowing any VM Operator to create any machine they wish, as this may cause security problems. Although the VM Operator may still perform actions that make the machine insecure later, at least we are starting with a set of VM images which have had some degree of security checking.

Another area of concern was the difficulty of detection and handling of security incidents in the EGI FedCloud. We have experienced a small number of security incidents showing the difficulty of detection. Incidents reported from FedCloud site A were pointing to compromised VMs at Site B. Site B operators did not have sensors/monitoring that would have detected the compromised VM. To mitigate this, we may have to deploy our own sensors at FedCloud sites. Discussions on this have just started, but the experience is all useful input to developing better handling, detection, and prevention.

Security risks arising from the proliferation of software and technology used in the Infrastructure are a concern, and threats arising from vulnerabilities and their handling have a high-risk value. Procedures in SVG have therefore been and are still being further modified to help address this.

EGI security team members are active in the WISE Information Security for Collaborating e-Infrastructures (https://wise-community.org/) including the Risk Assessment Working Group, where we can collaborate with others on the development of Risk management as applied to e-Infrastructures. See section 7 for more details.

3 New and revised EGI CSIRT/IRTF procedures and best practices

Providing operational security in an evolving distributed Infrastructure is a challenging task, consisting of the following elements:

1. Project-wide incident coordination and forensic support;
2. Vulnerability handling, and increasing the Infrastructure's resilience against standard attacks, by keeping the installed software up-to-date;
3. Policy and procedure development to address new technologies and services;
4. Training to improve the incident response capabilities of the participants;
5. Testing the incident response capabilities of the involved teams on all levels - Resource Centre, NGI, and Global/project level.

Each of these is now considered in turn in the following sub-sections.

3.1 Incident Response Task Force (IRTF)

The Incident Response Task Force (IRTF) has a crucial role in the overall provision of the operational security of the EGI Infrastructure. Most importantly this includes timely reaction to and handling of security incidents and IRTF also contributes to incident prevention by the handling of critical security vulnerabilities. The highly-distributed nature of both the Infrastructure and the IRTF adds another layer of complexity in this task, which can only be resolved by ensuring that proper procedures are in place and that these can easily be followed when time is of the essence.

For the coordination and resolution of incidents, all members of the EGI Infrastructure rely on the *EGI CSIRT Security Incident Handling Procedure*, also known as *SEC01*[4]. This procedure was modified in 2015 (and approved in 2016), following two main objectives. First, the introduction of cloud technologies introduced new capabilities (e.g. taking full memory and disk snapshots of a live VM) that could be used to improve forensic data retention, but also introduced new elements, indirections or opaque layers which had to be dealt with properly. This procedure update introduced new steps, taking advantage of these new capabilities but also requiring more data to be reported, to ensure full traceability. Secondly, while Virtual Organisations (*VOs*), and more generally users, have always been part of successful incident handling, their participation was not written into the procedure. Worse, the new virtualisation layer completely blinded sites, who became unable to observe or investigate user actions. As a result, this update included VOs and users directly in the new procedure.

At the same time as this public procedure was modified and while it was used to resolve incidents in 2016 and 2017, the internal procedures for IRTF have also been adapted. Each incident that

[4] https://wiki.egi.eu/wiki/SEC01

impacted the EGI Infrastructure during this period was later followed by a debriefing discussion, during which any imperfections of the incident handling could be identified and improvements discussed within the team. While most of these modifications were minor, not leading to major changes in the procedures, the accumulation of these changes and the enhancement of internal documentation have clarified the role, duties and capabilities of response duty coordinators, thereby improving the response capabilities of IRTF.

In addition, the EGI CSIRT is providing its constituents with guidelines in order to investigate and resolve incidents. In order to improve their immediate response and decrease forensic data losses, the EGI forensics guidelines (https://wiki.egi.eu/wiki/Forensic) have been updated and greatly improved. It now includes detailed steps to collect and analyse forensic information in the context of computer security but also provides configuration advice to increase the range of forensic data that can be collected and decrease data loss or alteration.

Concerning the prevention of incidents, in particular the resolution of critical vulnerabilities that could expose the EGI Infrastructure to a large-scale incident, the *EGI-CSIRT Critical Vulnerability Handling*, also known as SEC03 (https://wiki.egi.eu/wiki/SEC03), is the leading procedure. This procedure, well tested for conventional grid resources, did not require any extension to support the evolving Infrastructure. This procedure was, however, updated in 2015 to a more readable and accessible wiki format, indicating each step in readable tables and following the same model as for other EGI procedures. Moreover, the different timescales for each step have been clarified. The difficult and sometimes incompatible measures of time (7 calendar days versus 3 working days) have been replaced with straightforward incremental delays. While such a change might slightly increase the vulnerability patching delays, clear and predictable deadlines allow resource centres to properly align their own procedures. Last but not least, an additional step has been added to the procedure: running the EGI diagnostic tool, pakiti, manually on each affected node after their patching. This new step, which has been accompanied with a simplification of the deployment of pakiti on worker nodes, allows faster and simpler confirmation of the resolution of the vulnerability.

In response to the new concept of *Virtual Appliances*[5], which introduced certified configurations and was not covered by the existing procedures, an extension to SEC03 has been developed. Unfortunately, this new procedure, which required new communication endpoints and new interaction, has not been put into practice yet. The elements missing for its operational deployment have been identified and are currently being worked on by the responsible teams.

Procedures often have to rely on automated tools which can provide or simplify the various operations required by either a member of IRTF or more generally of the EGI Infrastructure. IRTF developed internal tools in order to decrease the number of repetitive tasks and to standardise the different messages sent. The EGI CSIRT has also adapted itself to the new EGI security dashboard, which exposed more information to EGI constituents but also added another source of

[5] https://wiki.appdb.egi.eu/main:faq:what_is_the_egi_applications_database_appdb

information. Such a transition required extra care, as differences between the sources and reports appeared and had to be fixed.

In order to improve the immediate isolation and containment of security incidents, the EGI CSIRT has been pushing for the wider deployment of a central emergency suspension solution. The manual suspension and manual reinstatement of identities involved in an incident by every EGI service operator has proven itself to be unreliable and leads to delays or partial results. A central solution has been deployed with a master record being distributed through each National Grid Infrastructure (NGI). In order to monitor this solution, a monitoring probe has been developed and used internally. It is currently under review before publication to be included in EGI's standard operational tests. While the initial deployment will be only for NGIs, it could easily be extended to sites that exposes their internal servers to the monitoring system.

3.2 Critical vulnerability handling

Keeping the Infrastructure patched and properly configured is key to its resilience against standard attacks. To properly handle critical vulnerabilities (see also section 6 - New and revised SVG procedures) the following steps need to be taken:

1. Analyse vulnerability and provide instructions to solve, or at least mitigate the security risk associated with the vulnerability in question in an advisory;
2. Targeted communication of the advisory to the affected resource centres;
3. Monitor the Infrastructure for vulnerable instances;
4. Follow up with Resource Centres running vulnerable instances.

The tools needed for this activity are based on standard software components extended with interfaces that allow for an efficient highly automatized vulnerability handling.

The required development of security monitoring tools together with the continuous production of monitoring probes for new vulnerabilities are carried out elsewhere in EGI-Engage (JRA1.4), in close collaboration with SA1.2.

3.3 Policy and procedure development

See sections 4 and 5 for the description of policy development. Procedures have been addressed in section 3.1.

3.4 Training to improve the incident response capabilities of the participants

The needed skills for proper incident response are usually beyond the experience of system administrators, in particular in specialised environments. In EGI it is crucial to have a deep

understanding of the technology to be able to use the available information for a more complete incident response. Security training is therefore of vital importance.

The training courses developed (in collaboration with EGI-Engage SA2.1) and offered to the participants are in 3 major categories:

- Defensive training. The participants are administrators of a virtual Site and have to defend against attacks performed by the trainers. The focus of this training is to detect anomalies in the system, understand the origin (attack vector) and communicate the results to trainers. The basis for these exercises are real incidents handled by EGI-CSIRT. The emphasis here is also to improve the forensic skills of the participants.
- Offensive training. Here the participant takes the role of an attacker and they are asked to attack a provided virtualised grid site with known vulnerabilities. The scope here is to demonstrate how attackers operate and how easy it is to compromise a system with information available on the internet. The target audience here are also the EGI FedCloud users that have to manage virtual machines.
- Role Play training. Here we created a "what if" situation and looked at possible incident response problems when new technology is part of an incident. Here we can look at the collaboration not only of the security teams but also involve management, press officer etc in the process.

During EGI-Engage to date we have run 10 security training events with ~20 participants each on average.

3.5 Test the incident response capabilities of the involved teams at all levels

The incident response capabilities of the security teams active in EGI at all levels (Resource Centre, NGI, Global/project level) are tested with Security Service Challenges (SSCs). Here we create a realistic scenario of an incident spreading in the Infrastructure and let the teams use their incident response tools. Not only the effectiveness of the deployed centralized incident response tools is tested but also the response procedures and EGI policies are also checked to confirm that they support an efficient incident response.

Plans for an enhanced security challenge framework for the EGI FedCloud were agreed by the EGI CSIRT. The framework has been developed and is ready and running and has been tested at a number of sites. More work, however, is required in the usage of contextualisation and configuration of EGI FedCloud sites before a full challenge can be run.

4 New and revised security policies

Several new security policies have been produced and many others have been revised and updated during the EGI-Engage project. These changes were made to properly address issues related to the evolution of EGI services and technology and to mitigate risks identified in recent security risk analyses. The development of new security policies includes detailed work inside the EGI Security Policy Group (at face-to-face meetings, by e-mail and by video conference). It is important to consult widely on the new documents and to take feedback into account. This consultation included presentations and discussions at the regular series of EGI conferences and also in the more frequent meetings of the Operations Management Board and of the EGI FedCloud group.

To start the policy activities a two-day face-to-face meeting of the EGI Security Policy Group was held early in March 2015. At this meeting agreement was reached as to which security policies were the most important for attention during the first year. Work started on four new or revised policies during the meeting and continued during PY1.

An updated version of the "Acceptable Use Policy" was produced and circulated widely for comments. This version was generalised to include all EGI service offerings (HTC, Clouds, EGI Science Applications on-demand Infrastructure, a.k.a. Long Tail of Science, etc.). At the same time wording was changed to require appropriate acknowledgement of the use of resources and support received in publications. It also addressed issues of liability. Work on a new Data Protection policy framework highlighted that yet more changes were required to the AUP before seeking formal adoption, which delayed the adoption of the new AUP until PY2.

A revised "Security Policy for the Endorsement and Operation of Virtual Machine Images" was produced using input from a better understanding of the usage of VMs in the EGI FedCloud. This revised policy included changes to responsibilities and trust to better fit the EGI FedCloud. Reaching agreement on the content of this policy and working with the EGI FedCloud group on the requirements for the technical implementation of the image endorsement in the EGI AppDB took some time so formal approval only happened in PY2.

A new draft policy and guidelines document entitled "The EGI Science Applications on-demand Security Policy" was produced, in collaboration with SA1.3. The policy (which used to be known as the Long Tail of Science scoped security policy) aims to enable a low-barrier service to be offered to a wide range of research users in Europe and their collaborators world-wide, by any Resource Centre organisation that elects to do so. In offering such EGI Access Services, the Resource Centre shall not negatively affect the security or change the security risk of any other Resource Centre or any other part of the Infrastructure. The document also provides guidelines on the implementation of security procedures and controls. A version of the new EGI AUP specific to the EGI Access Service was also produced and adopted.

The final policy worked on during the first year, was a complete revision of the policy on Data Protection. This new policy ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of these data, for example those relating to user registration, monitoring and accounting contains “personal data” as defined by the European Union (Directive 95/46/EC). The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals. This policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.

Security policy development work in the second year of EGI-Engage included a full revision of the top-level Security Policy document to make it more general and more obviously applicable to all current and new EGI services. Work on this was completed during a face-to-face meeting of the EGI SPG in November 2016 and after consultation the revised document was formally adopted in February 2017.

A policy on Acceptable Authentication Assurance was produced and also adopted in February 2017. This policy is an update of the old security policy "Approval of Certification Authorities". It was updated to cover the current Interoperable Global Trust Federation (IGTF) levels of assurance and other changes. This policy defines the approved authentication assurance sources.

During 2016, all remaining old security policies, except those related to VO management, were updated to make them more general and to use new glossary terms for the current and evolving EGI services. There was no change to the policy content of the documents. The specific policies updated were:

- The VO Portal Policy
- The Policy on e-Infrastructure Multi-User Pilot Jobs
- The Security Traceability and Logging Policy
- The Security Incident Response Policy

The three policies on VO management will be updated during the last 6 months of the project (see section 8.3).

The full list of currently adopted security policies is always available on the EGI policies and procedures wiki at https://wiki.egi.eu/wiki/Policies_and_Procedures.

The EGI Security Coordinator has been leading the WISE SCIV2-WG, where work is ongoing on version 2 of the Security for Collaborating Infrastructures trust framework. The aim here is to broaden the number and type of stakeholders involved by including GÉANT and perhaps some NRENs. The SCI version 1 document has been studied to see which components are no longer needed, to check for missing issues and to reword to meet the requirements of the broader set of stakeholders. A good draft of version 2 was produced during the WISE workshop in Nikhef in March 2017.

5 The evolution of trust and policy in AAI & federated identity management

The work reported here has been carried out in collaboration with EGI-Engage JRA1.1 and the AARC project (EU H2020).

The Interoperable Global Trust Federation (IGTF) is the primary source of identity assurance level specifications in use within the EGI Infrastructure, and EGI maintains a dedicated liaison membership in the IGTF to support its policy and engagement evolution with the EGI user communities. The IGTF is a joint effort that permits global federation of identities and trust, aligning identity assurance requirements also for PRACE (the Partnership for Advanced Computing in Europe), XSEDE and the Open Science Grid in the US, HPCI (the High Performance Computing Infrastructure in Japan), and a large number of national e-Infrastructures.

The EGI-IGTF liaison function is visible to the resource centres and users primarily by way of the single 'trust anchor distribution': a set of roots of trust that all met or exceed defined minimum requirements. This distribution remains a key responsibility of the liaison function, which also supports the IGTF in this role, and from the start of the EGI-Engage project until April 2017, in total 18 releases were distributed to the EGI Infrastructure. Yet the scope and range of the trust anchors is continuously evolving. Based on a global user requirements analysis with the Research and e-Infrastructures, the IGTF introduced multiple assurance *profiles*: combinations of assurance elements, structured according to the OGF CAOPS-WG *Authentication Service Profile* (https://redmine.ogf.org/dmsf_files/29?download=), that combine identity assurance elements into a limited set of combined profiles (https://www.igtf.net/ap/authn-assurance/) that match specific Infrastructure risk profiles. Three of these ("ASPEN", "BIRCH", and "CEDAR" – non-hierarchical naming is used to identify the profiles) all correspond to approximately the same level, but using different underlying authentication technologies: respectively local site, R&E (inter) federation, and end-user-based. In addition, an 'identifier-only' trust assurance level was introduced ("DOGWOOD") that provides persistent non-reassigned identifiers to all entities, alongside a revocation-, freshness-, and traceability capability, but does not convey identity information (names, affiliation) by itself.

The key benefit of this approach is that it allows distribution of authentication responsibilities between identity providers, research communities, and resource centres. Several structured user communities (WLCG, ELIXIR, but also the EGI Access platform through its delegated enrolment scheme) by themselves collect identity data, and require from the authenticator no more than the guarantee of uniqueness (non-reassignment). This brings a new level of flexibility to the EGI trust management system: users are not required to register twice, and the enrolment flow can be simplified. It introduces a *combined assurance ('combined adequacy')* model, where the

combination of identity data from the home organisation (typically a federated organisation in an existing national R&E identity federation) with identity data held by the structured user community provides sufficient means to answer the basic security questions *who, what, where, and when*, and permits access control decisions to be made.

The model was piloted with the four user communities from the LHC experiment by way of a specific trust anchor (the "CERN WLCG IOTA CA") using existing mechanisms in the *Policy on Approval of Certification Authorities* (described in the *Considerations on the coexistence of controlled and flexible community models*, https://documents.egi.eu/document/2745), pending the necessary software support by the EGI technology providers. Following successful testing, this mechanism was formalised in the *Policy on Acceptable Authentication Assurance* (https://documents.egi.eu/document/2930) which lays down the requirements on the joint assurance level. The work in EGI and the IGTF was carried out in in close conjunction with the AARC project and the REFEDS community. The evolution of the assurance trust framework in particular permits the integration of the *RCauth.eu* AARC pilot service, which provides a CILogon-like token translation service for Europe.

The pilot service was connected to the EGI trust framework in a controlled way, since secure introduction of the new class of 'identifier-only' trust services requires simultaneous deployment and configuration of authorization software components. This is technically achieved by the introduction of a supplementary trust anchor package ("egi-policy-cam", reflecting the *combined assurance/adequacy model* name) and made available to the resource centres in March 2017 for controlled testing (http://repository.egi.eu/sw/production/cas/1/preview/). Wider adoption will be recommended to the service administrators once authorization software support has been fully deployed. Meanwhile, the mechanism is used by selected user communities in EGI (WLCG, ELIXIR) and in some constituent NGIs (e.g. in NGI-NL for support of the *Project MinE* on ALS research) based on the EGI IGTF package distribution.

Other trust issues related to federated identity included input to the work on the Sirtfi activity of REFEDs (https://refeds.org/sirtfi), which is building a trust framework for security incident response in the identity federations in collaboration with the AARC project.

6 New and revised SVG procedures

The purpose of the EGI Software Vulnerability Group (SVG) is "To minimize the risk to the EGI Infrastructure arising from software vulnerabilities". This is an important activity as some of the threats with the highest risk value concern threats due to software vulnerabilities. The biggest way in which this has been enacted has been through handling software vulnerabilities which are reported and are relevant to the EGI Infrastructure. Handling software vulnerabilities is an important part of incident prevention, reducing the security risks to the Infrastructure.

Towards the end of 2015 the EGI SVG carried out a major revision of the Software Vulnerability Issue handling procedure to address the evolving EGI services. The revised version is at https://documents.egi.eu/public/ShowDocument?docid=2538. The main purpose of this document is to describe the EGI Software Vulnerability Group issue handling procedure, including how to report a vulnerability, which steps are carried out, and the responsibilities of the various parties involved. All types of software vulnerability which are relevant to EGI are handled, which includes software vulnerabilities both 'discovered' in software, usually in software developed by persons collaborating with EGI to enable the secure sharing of resources, as well as vulnerabilities announced by software providers. In addition, it briefly describes other strategies for minimizing the risk to the EGI Infrastructure due to vulnerabilities.

Previously during EGI-InSPIRE the main focus of SVG was on handling vulnerabilities in Grid Middleware, and EGI CSIRT handled vulnerabilities in the Linux operating system. In recent years, the proliferation of different types of software on the Infrastructure has meant that EGI has had to revise the procedure and strategy for handling vulnerabilities. In EGI-Engage it was decided to have one group to handle all vulnerabilities, and members of EGI CSIRT who take a duty as the 'Security Officer on Duty' are now all members of SVG. The 'Security Officer on Duty' therefore also sees all information on vulnerabilities reported to SVG, and if they wish to take urgent action to protect sites then they may. The major revision of the EGI Software vulnerability issue handling took this into account. In addition, the revision took into account the reduction in homogeneity of the EGI Infrastructure, and changing technology including the EGI FedCloud.

The Vulnerability handling procedure is now as follows:

- Anyone may report a vulnerability, by e-mail to report-vulnerability@egi.eu This may be to report a vulnerability discovered in software, or to alert SVG to a publicly announced vulnerability which may be both relevant and a concern to EGI.
- SVG, along with the reporter and if appropriate the technology provider investigate the relevance and effect of the vulnerability in EGI.
- If the issue is valid and relevant, a risk assessment is carried out where the vulnerability is placed in one of four risk categories - Critical, High, Moderate or Low.
- If the vulnerability has not been fixed, a target date is set according to risk.
    - For 'Critical' - special process is carried out according to the circumstance
    - High - 6 weeks
    - Moderate - 4 months
    - Low - 1 year.
- This target date is the date by which software free from the vulnerability should be available for installation in all appropriate repositories. This allows the prioritization for the timely fix of software vulnerabilities.
- An advisory is issued:
    - If EGI SVG is the main handler of vulnerabilities concerning this software, regardless of the risk

        - When it is fixed
        - On the Target date if it is not fixed by then
    - If the issue is assessed as 'High' or 'Critical' risk
    - If the EGI SVG considers it useful to alert sites

Since the advent of the EGI FedCloud, consideration of vulnerabilities in software enabling the EGI FedCloud as well as software included in virtual machines has to be considered. Cloud enabling software is handled in a very similar way to Grid enabling software. Software in Virtual Appliances presents new challenges, which are not fully addressed in the current procedure. If a critical vulnerability is found related to a Virtual Appliance, then this needs to be updated urgently by those responsible for the virtual appliance.

A wider range of software and technology is being used in EGI than it was in the past, and it is not reasonable to expect there to be good expertise on all the technology used in EGI within the software vulnerability group. SVG cannot control what software is used in the EGI Infrastructure. Hence, we rely more on the software providers to analyse vulnerabilities in cases where there isn't the expertise in the group, and vulnerabilities are handled more from a procedural point of view.

One addition to help with the greater proliferation of software is to ask those who develop or select software to consider security and maintainability. To help this we produced a Software Security Checklist, which at present consists of 10 points which people should consider when developing or selecting software to avoid some of the common problems from which vulnerabilities arise or which make it difficult to address if they do. This list has also been placed on the wiki (https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist).

The actual operational software vulnerability issue handling is not funded by EGI-Engage, but it is of interest to state the number of issues handled during the 2 years since the start of EGI-Engage. Between 1st March 2015 and 31st March 2017, 98 vulnerabilities have been reported and handled by SVG. During that time 55 advisories have been issued including for 12 which were assessed as 'Critical' risk and 23 assessed as 'High' risk. The types of software where issues are reported has changed. Of the 98 potential vulnerabilities handled 19 concerned Grid Middleware. 16 concerned cloud enabling software, and 10 concerned the Linux kernel.

7 Information Security Management - collaboration with other e-Infrastructures and Research Infrastructures

The EGI-Engage project takes a leading role in the coordination of Information Security management for e-Infrastructures. Following on from initial discussions at the EGI Conference in

Lisbon in May 2015 we (EGI Security and a PDO from the GÉANT Amsterdam office) decided to pursue the possibility of enabling the Security for Collaborating Infrastructures (SCI) activity, chaired by the EGI Security Coordinator, to meet jointly with the newly formed SIG-ISM activity of GÉANT. This SIG acts as an information exchange forum to discuss standards and best practices for Information Security in the NRENs. It was recognised that there could be great benefits in the e-Infrastructures and NREN communities working closer together on security topics of common interest. Further discussions in June 2015 created a small programme committee for what became "The First WISE meeting" in Barcelona on 20-22 October 2015. Approximately fifty people in total attended made up of representatives of the EU e-Infrastructures (EGI, EUDAT, GÉANT and PRACE) together with representatives of many NRENs, participants from the USA (XSEDE, NCSA, CTSC) and communities like LIGO, HEP/CERN, Human Brain Project and others.

WISE stands for "Wise Information Security for Collaborating E-infrastructure" and is a global trust community where security experts share information and work together, creating collaboration among different e-infrastructures. WISE provides a framework of standards, guidelines, and practices to promote the protection of critical infrastructure.

The first meeting was a success and it was agreed that we would continue to work together, meet face to face twice a year and, in the meantime, make actual progress in a number of working groups. The EGI Security Coordinator is co-leading a working group called “SCI-V2WG" which will take the SCI Version 1 document forward to include more stakeholders, e.g. NRENs, in the defined Trust Framework. EGI will wherever possible also be active in other working groups; Risk Analysis, Security in Big Data/Open Data, Review and Audit, training and awareness. Members of the EGI security team will also continue to serve on the WISE steering committee.

Further meetings of WISE were subsequently held at the XSEDE meeting in the USA in July 2016, at the Digital Infrastructures for Research Conference in Krakow in Sep 2016 and then hosted by Nikhef in Amsterdam in March 2017.

Through its broad representation in the steering committee, EGI can benefit from better alignment of security practices and increased input into its risk assessment, training and trust programmes. The construction of comparative policy frameworks allows easy movement of researchers and data across multiple Infrastructures, whilst the construction of the human network through periodic WISE workshops (twice-yearly) established communications channels also for operational security activities.

8 Future plans

In this section, we present the plans for the remainder of EGI-Engage, i.e. the last 6 months of the project. We divide the plans into the same 5 sub-tasks as before.

8.1 Plans: Security requirements and risk assessment for new services, technology, and deployments

A general review of the security risk assessment will be carried out, to assess the status of mitigation of the risks and where we may have missed threats to the EGI environment. Three more threats having a high-risk value will be reviewed in detail, the mitigations currently in place considered and further mitigations recommended.

In the EGI FedCloud, we will push for wider deployment of the VM Operator role, i.e. individuals who can instantiate VMs and then have responsibility for the security of those running VMs. At present, there are many VOs where any of their members can instantiate VMs. This has implications both for giving VOs control over who can do what, and security implications if persons who do not have sufficient knowledge concerning the secure operation of VMs are able to instantiate VMs.

EGI representatives will continue to be active in the WISE Risk Assessment Working Group. This joint collaboration on defining best practice in security risk management will help EGI and other Infrastructures perform more effective risk assessments in the future.

8.2 Plans: The evolution of operational security procedures, including forensics

The existing security procedures have to constantly evolve to address specific issues resulting from the use of new technologies. These are not limited to Cloud technology but also have to cover modified or newly introduced VO workload management systems.

We plan to review the relevant security procedures (SEC-01, SEC-03, SEC-05) and update them where necessary before the end of the project.

As a result of the planned SSCs (see section 8.4) we also have to further develop our forensics toolsets to address new challenges in that field introduced as a result of a changing environment. The elements missing for operational deployment have been identified and are currently being worked on by the responsible teams.

8.3 Plans: Develop a new trust framework and develop new policies

We plan to revise all existing security policies related to VO management, i.e. user registration processes and the secure operation of user communities, including the management of their membership database. This includes aspects arising from the relationship between user communities and the EGI Infrastructure and also the relationships between communities and their individual users. We plan for two security policies, one to address each of these aspects.

In order to support the combined assurance model and alignment with R&E identity federations, we will develop the requisite processes for assessing combined adequacy of the community identity management. Wider adoption of the existing pilot service will be recommended to the service administrators once authorization software support has been fully deployed.

Version 2 of the WISE Security for Collaborating Infrastructures Trust Framework will be finalised and published. There are plans for a signing ceremony and endorsement of SCIV2 at the TNC17 conference in Linz in June 2017.

In relation to the sustainability of the security policy and trust area after the end of EGI-Engage, all of the important bodies will continue to exist; EGI Security Policy Group, IGTF, EUGridPMA and WISE. The existing EGI security team staff also all plan to continue working on these activities. We see a growing requirement in future to develop and maintain trust and policy frameworks which are useful to the broadest possible range of e-Infrastructures and Research Infrastructures. WISE and IGTF will therefore continue to be two important bodies where such issues can be worked on and agreed. The staff and institutes currently involved in these activities will continue to seek ongoing support and funding from the EC, from NGIs and from other sources of national and institute funding.

8.4 Plans: Develop the security challenge framework

The Security Service Challenge framework will be further developed to allow for either a full assessment of EGI FedCloud's readiness to respond to an incident affecting multiple Resource Centres or for an assessment of the Infrastructure's readiness to respond to an incident affecting the DIRAC job submission system. We do not have the effort or time available to run both SSCs before the end of EGI-Engage. We are currently assessing which of the two options to choose.

8.5 Plans: Develop the software vulnerability handling process to adapt to new technology and deployments

There are plans to make further updates to the SVG issue handling procedure before the end of EGI-Engage. These include updates needed to address the continuing reduction in homogeneity in the Infrastructure deployment and configuration, and further technological changes. This also includes possible improvements to the definition of the various risk categories. In some cases, SVG informs sites to check the configuration of certain pieces of software, where a poor configuration may leave a site vulnerable. In these cases, we do not necessarily include a risk category, and this situation will be added to the procedure. The handling of some recent vulnerabilities is being reviewed. These are being treated rather like use cases in order to improve the vulnerability handling procedure. In particular, the handling of 'Critical' vulnerabilities is being updated where this is not an easy solution or patch.

EGI FedCloud uses endorsed VM images on which the running Virtual machines are based. We plan to clarify the vulnerability issue handling procedure and responsibilities where vulnerabilities relevant to endorsed VM images and running Virtual Machines are found. In particular, if an endorsed VM image is based on a vulnerable kernel, it is important that the VM image has its endorsement removed and the image is replaced in a timely manner, according to the severity of the vulnerability. Improved mechanisms for contacting the relevant VM endorsers and VM operators (which operate the running Virtual machines) are planned as part of the improvement of this process. This includes creating mailing lists for those who generate and endorse VM images, and for those who operate Virtual Machines.

We are continuing to pursue better collaboration with other distributed Infrastructures, such as EUDAT, OSG and CTSC. This should allow greater efficiency in dealing with vulnerabilities and exchanging information on vulnerabilities relevant to other distributed computing Infrastructures.

9 Plan for Exploitation and Dissemination

This section provides a plan for exploitation and dissemination (PEDR) of the project results documented in this deliverable. The content will be used to update the catalogue of project results (http://go.egi.eu/egi-engage-results) and to develop an overall PEDR for the whole project.

Name of the result	Evolution of EGI operational security
DEFINITION	
Category of result	• **Policy & Procedure developments**: Technical procedures directed at users, service and infrastructure providers (for example to govern access and allocation to resources), policy reports and recommendations, and strategic analysis • **Know-how**: Includes all results from fact-finding activities (e.g. surveys, requirement gathering), but also the results from internal exercises (e.g. security challenges) and outputs that can be used for knowledge transfer as training materials.
Description of the result	Evolution of EGI security policies, procedures and best practices to mitigate the security risks arising from new trust models, new technology and new services deployed in EGI. IGTF trust developments enabling the EGI AAI platform that allows the integration of service providers with identity federations.
EXPLOITATION	
Target group(s)	Research communities, Research Infrastructures, EGI Operations, EGI FedCloud

	resource providers, AAI users, resource Providers, NGIs, and the EGI CSIRT.
Needs	Everyone requires secure and available services. Users and research communities need uniform authentication and authorization workflows to reduce the overhead on the service providers and users.
How the target groups will use the result?	The target groups inside the EGI domain will be required to use the new security policies and procedures once formally adopted. The new policies and procedures will be made available to other e-Infrastructures and Research Infrastructures through WISE and via the EGI web site as example of best practice
Benefits	Increased security and availability of services and data
How will you protect the results?	The new security policies and procedures are published with a Creative Commons copyright Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/)
Actions for exploitation	New security policies and procedures are published on the EGI web site once formally adopted.
URL to project result	https://wiki.egi.eu/wiki/Policies_and_Procedures
Success criteria	EGI participants abide by the new policies and procedures. Security incidents are either avoided or more effectively contained, and services and data remain available.
DISSEMINATION	
Key messages	The new security policies and procedures will provide better security of and higher availability of EGI services and data
Channels	EGI meetings (OMB etc.), EGI conferences, EGI web site.
Actions for dissemination	Presentation at the EGI & Indigo conference in Catania (May 2017)
Cost	Attendance costs and preparation time for 5 members of the security team
Evaluation	EGI participants abide by the new policies and procedures. Security incidents are either avoided or more effectively contained, and services and data remain available.