EGI.eu

EGI Federated Cloud Security Questionnaire for Cloud Resource Providers deploying Cloud technology

Document identifier	EGI_CSIRT_SVG_FederatedCloud_CRP
Document Link	https://documents.egi.eu/document/2114
Last Modified	25/07/2014
Version	0.8
Policy Group Acronym	CSIRT
Policy Group Name	Computer Security Incident Response Team
Contact Person	Linda Cornwall, Sven Gabriel, David Groep
Document Type	Procedure/Questionnaire
Document Status	Draft
Approved by	OMB?
Approved Date	DD/MM/YYYY

Policy Statement

This is a checklist for Cloud Resource Providers (CRPs), which must be answered by CRPs to provide the minimum information which CSIRT requires to consider whether to recommend CRP Certification from a security point of view in order to be part of the EGI infrastructure, in particular the EGI Federated Cloud. This document is now a reference document. Sites should fill in the questionnaire either online at

https://www.surveymonkey.com/s/Cloud_Security_Questionnaire_for_Resource_Centres

or the editable PDF provided in this document link.

I. AUTHORS LIST

	Name	CSIRT	Date
From	Linda Cornwall, Sven Gabriel, Daniel Kouril, Maarten Litmaath, David Groep, Malgorzata Krakowian		25th July 2014

II. DELIVERY SLIP

	Body	Date
Reviewed by	TCB	DD/MM/YYYY
Reviewed by	OMB	DD/MM/YYYY
Reviewed by	UCB	DD/MM/YYYY
Approved by	EGI.eu Director	DD/MM/YYYY
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Version	Date	Comment	Author/Organization
0.1	14th Feb 2014	First Draft after various e-mail discussions	Linda Cornwall/STFC
0.2	18th Feb 2014	Second Draft, mainly David Group's work, and Maarten's changed	Linda Cornwall/STFC David Groep Maarten Litmaath
0.3	25th Feb 2014	Comments from Stephen Burke and Oxana Smirnova addressed	Linda Cornwall/STFC
0.4	7th March 2014	Comments from Alvaro Lopez Garcia (partially addressed)	Linda Cornwall/STFC
0.5	31st March 2014	Added tables in appendix A, plus sentence on privacy to 2.4.	Linda Cornwall/STFC
0.6	24th April 2014	New version after filled in by first person/site to try it (Alvaro Lopez Garcia) followed by discussion at the EGI CSIRT F2F meeting.	Linda Cornwall/STFC
0.7	25th July 2014	Now has been converted to survey and editable PDF by Malgorzata Krakowian. This document is edited to match numbering and be used as a reference.	Linda Cornwall/STFC
0.8	25th July 2014	Minor change to separate 1 question into 2	Linda Cornwall/STFC
1.0			
2.0			
3.0			
4.0			

IV. APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

VI. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

- Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
- Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
- Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities
- Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI will collect user requirements and provide support for the current and emerging user communities. 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 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, 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 − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 INTRODUCTION

The EGI infrastructure has been based on Grid Technology for more than a decade, and the Grid based technology is very mature from a security point of view. The various EGI security teams, Computer Security Incident Response Team (CSIRT), the Software Vulnerability Group (SVG), and the Security Policy Group (SPG) have been working to develop policies and techniques to allow the secure sharing of computing resources across a global infrastructure. It is important that this experience is applied and adapted to newer technologies, and at present this in particular means 'Cloud' technology.

1.1 EGI Security Policies apply in the Cloud

Resource Providers deploying Cloud technology should be aware that the security policies developed by the EGI Security Policy Group (SPG) apply to any technology, including Cloud technology, which is deployed in the EGI infrastructure. These policies are listed at [R 1]. These policies may require some adaptation to cope with changing technology, and changing responsibilities of the various participants in the infrastructure.

1.2 Security principles continue in the cloud

Just because technology is changing, does not mean that security principles change. It is still necessary to ensure that Resource Providers are run in a secure manner, and that data access is properly authorized, credentials are protected, and that it is possible to carry out incident response and suspend a user or identity which is involved in a security incident. This means suitable traceability of users and contacts for the Resource Providers are in place.

1.3 Security is evolving

Any checklists or recommendations produced will evolve over time, as experience with new technology develops and becomes better understood and as technology changes.

1.4 Caveats

This is the minimum requirements concerning Federated Cloud Services which the EGI CSIRT team considers necessary to recommend certification. This is the first version, and it defines the minimum we have identified as being necessary at the present time. It is subject to revision, future Resource Providers seeking certification may be asked for more by the security team and service providers already certified may be asked to put more controls in place in the future.

1.5 Filling in the survey

Sites may fill in the on-line survey at

https://www.surveymonkey.com/s/Cloud_Security_Questionnaire_for_Resource_Centres

Or fill in the editable PDF version supplied with this document.

Note that all questions up to and including question 18 need to be answered, questions 19 to 25 are only applicable if you are running customer VMs from customers that are not controlled through EGI security policies.

If sites fill in the on-line survey, in order to move onto the next page they need to answer all questions on a particular page. It is possible to put 'junk' in the survey, and go back to the previous page. It is also possible to return to the survey if you are using the same computer as before.

If the editable PDF is used should be sent to irtf@mailman.egi.eu after it is complete.

1.6 This document is now for further information

This document is largely replaced by the survey. But it is kept as in many cases it includes more detailed explanations, if people want more information.

2 QUESTIONNAIRE FOR SITES DEPLOYING CLOUD TECHNOLOGY

This survey contains the basic security related checks which must be carried out with Cloud Resource providers (CRP) offering "Infrastructure-as-a-Service" clouds based on the execution of virtual machine images. This is in order for EGI CSIRT to be satisfied that the Resource Providers is suitable for inclusion in the EGI Federated Cloud. This does not include checks that other required mechanisms are in place, such as for accounting, which are also necessary for the Certification of a Federated Cloud Resource Provider.

The survey is divided in following parts:

1. General information
2. About the Cloud Resource Providers (mandatory)
3. About the Cloud services provided (mandatory)
4. About the virtual machines instantiated in the cloud (mandatory)
5. About EGI and nonEGIcotenancy

(Not applicable if only EGI FedCloud VMs are used.)

This survey is a part of Resource Centre certification procedure and this is a mandatory step to join EGIProduction Infrastructure.

2.1 General Information

This is section 1 in the survey

2.1.1 Please provide Name and contact details

(Name and e-mail address)

This is question 1 in the survey

2.1.2 What is your role in the resource centre?

This gives the choice of Site Operations manager, Site operations deputy manager, site security officer, or site administrator

This is question 2 in the survey

2.1.3 Please provide the resource centre name you are representing

I.e. the site you ae referring to in this survey

It should be the same as it is registered in the GOCDB (http://goc.egi.eu)

This is question 3 in the survey

2.2 About the Cloud Resource Providers

This is section 2 in the survey

2.2.1 Check that CSIRT email is set in the GOCDB, and that it works, and provides a response.

The Resource Provider should confirm that the CSIRT e-mail for their site is set in the GOCDB [R 6]. This should be a generic address, rather than an individual.

This is important as it this is the e-mail address which is used to handle incidents, as well as being the address used to send alerts and advisories.

CSIRT should check that this works, and produces a response.

This is question 4 in the survey

2.2.2 The Cloud enabling technology used

The software stack(s) used to provide the federated cloud service must be described. This may be, for example, OpenStack or OpenNebula.

Where proprietary software is used, it is RECOMMENDED to ask for a security assessment thereof to be provided. The CRP MUST agree to discontinue products that are known to pose a security threat to the Infrastructure, as determined by the EGI Security Teams – or at its option withdraw from the infrastructure.

This is question 5 in the survey

2.2.3 What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?

This is question 6 in the survey.

2.2.4 Describe the network separation of management and service traffic.

This includes aspects such as: presence of a separate network for management of physical hosts and the (virtual) network(s) to which customer VMs can be connected; whether that is a physically separated network; what are the (network) security controls separating the management network from the systems running the cloud enabling software; can customer traffic be separately monitored?

There probably is a range of 'right' answers, but it should allow for containment of incidents, and monitoring of traffic in a way that preserves confidentiality of non-affected customers, &c.

This is question 7 in the survey

2.2.5 Do you agree to be bound by the EGI security and other policies

See [R 1].

This is question 8 in the survey

2.2.6 What processes exist to maintain audit logs (e.g. for use during an incident)?

If there is a standard way which EGI Federated cloud recommends, these mechanisms may be used. In general, outbound connections must be logged and traceability must be ensured (EGI may provide a general instructions for CRPs on how to configure this).

This is question 9 in the survey

2.3 About the Cloud Services Provided

This is section 3 in the survey

2.3.1 Who is allowed access to the management of the cloud services, and how do they obtain access?

The CRP should state who has access to managing the cloud enabling system, including the hypervisors.

This is not about the virtual machines.

This is question 10 in the survey

2.3.2 Are the cloud-enabling services run on a dedicated system to which only cloud customers have access, or are services also offered through other interfaces?

This is primarily about whether there are other forms of access, rather than through the Federated Cloud access mechanisms. State how this access is obtained.

This is question 11 in the survey

2.3.3 State whether identity providers other than EGI-approved are enabled?

For identifying users, EGI maintains a policy regarding the trusted Certification Authorities for use in EGI [R2]. If you support authenticating VM operators with other types of identity than those approved by EGI, please state both their type and identity assurance level. Describe how appropriate traceability to the end-entities involved is retained through these identity mechanisms (one may take the classification of the EGI VO Portal [R 3] as an example).

If you allow external third parties to manage system entities other than VM images (and image store etc.), describe how they are authenticated.

It is understood that it may not be possible to describe this for non-EGI customers. It is essential that this is described for any action which may be attributed to an EGI related entity.

This is question 12 in the survey

2.3.4 Is it possible to suspend a User or group of users?

EGI produces a list of DNs under central security emergency suspension, [R 5] where DN(s) may be suspended due to a compromised identity certificate or ongoing incident.

State whether the CRP is able to take this information provided centrally by the EGI security teams and suspend users.

This is question 13 in the survey

2.3.5 If Q13 Yes, please state how suspensions are effectuated with regard to currently executing VMs.

This is question 14 in the survey

2.4 About the Virtual Machines instantiated in the Cloud

This is section 4 in the survey

2.4.1 Image sources and the EGI Federated Cloud model

For EGI users, does the CRP follow exclusively the EGI Federated Cloud model of running 'endorsed' virtual machines from a trusted EGI market place? See the EGI policy for the Endorsement and operation of Virtual Machines. [R 4].

This is question 15 in the survey

2.4.2 What mechanism is in place to ensure only endorsed VMs are executed on the infrastructure?

Which controls are used to ensure this is applied for all VMs? Which mechanisms are used to ensure VMs in the local image store are all endorsed and no non-endorsed VMs are executed?

This is question 16 in the survey

2.4.3 Differentiating operators and users

Can and does your cloud management framework separate operators (those with responsibility for the security of the VM, typically having root access to the VM, see definition in [R 4]) and users? If so, do you apply different controls for each of these groups?

This is question 17 in the survey

2.4.4 Network monitoring

Describe how network monitoring is implemented for customer VMs. Describe how all network traffic can be traced to a specific VM instance and its associated operator. If the user has root to the VM, can you confirm that the user's connections are still monitored externally to the VM.

This is question 18 in the survey

2.4.5 Incident response and investigations

Describe your ability to participate in incident response and investigation.

Are you capable of preserving point-in-time snapshots of the state of a virtual machine executing in your infrastructure? Are you allowed and willing to share the images related to EGI FedCloud users and user communities with the EGI security incident response team(s)? Do you have any preconditions related to investigations and incident response?

This is question 19 in the survey

If only EGI FedCloud VMs are used, the following questions are no longer relevant. Many of the questions below should then be addressed by the VM endorsers and/or the VM operators, who are subject to their own policy sets.

2.5 About EGI and non-EGI co-tenancy

This is section 5 of the survey

You (also) run customer VMs from customers that are not controlled through EGI security policies. This could potentially pose a risk to the EGI FedCloud infrastructure, other CRPs, VM operators, or end-users (e.g. because actions are ascribed to EGI users who are not involved in an incident, or because data integrity or confidentiality of EGI users is compromised). For the EGI security teams, it is important to be able to assess the associated risks.

While we understand that due to privacy issues with some customers, you may not be able to give full answers to all questions; it is important to explain how you ensure that the co-tenancy does not give rise to security problems for EGI and that actions from other users cannot interfere with or be incorrectly associated with EGI users. Please provide as much information as possible to allow judgement as to whether we can have confidence in the operation and separation of these services.

2.5.1 How do you ensure that the co-tenancy does not give rise to security problems for EGI and that actions from other users cannot interfere with or be incorrectly associated with EGI users?

This is question 20 of the survey

2.5.2 How are your non-EGI customers identified? Can these users be authenticated and positively distinguished from EGI users? What mechanisms are in place to ensure actions are not inadvertently associated with identified EGI users?

How (if so) are EGI and non-EGI customers separated? How (if applicable) are EGI customers protected from other tenants?

This is question 21 of the survey

2.5.3 Policies

Do you require that all customers abide by a set of security policies and/or do you have an acceptable use policy (AUP)? Are your terms and conditions publicly available (and if so, where)?

Describe what communication mechanisms are in place to ensure your customers are aware of these policies, terms and conditions.

Do your terms and conditions protect customers from each other?

Does your AUP include clauses that permit participating in incident response by, e.g., providing network and systems information? Would you consider the EGI security incident response task force forensics expert(s) as an appropriate third party in such investigations, when they pertain to incidents involving EGI users, VM operators, and/or VM endorsers?

This is question 22 of the survey

2.5.4 VM execution

Are all non-EGI customers able to execute VM images?

Which VM operators do you allow? See definition in [R 4]

This is question 23 of the survey

2.5.5 Process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?

Do your terms and conditions or AUP put requirements on the VM images with regards to vulnerability patching?

Do your terms and conditions or AUP put requirements on the external behaviour of the VMs executing (such as: no security violations, no network abuse nor spoofing, no email or message abuse, &c)?

Do you have systems in place for the enforcement or monitoring that (non-EGI) customers comply with these policies?

This is question 24 of the survey

2.5.6 If a non-EGI customer(s) are implicated in a security incident, are you able to suspend/prevent their usage of the system?

This is question 25 of the survey

2.5.7 How long are identity and audit records for Non-EGI customers retained?

If an incident occurs, which may be due to a non-EGI user, then retention of logging and your ability to investigate an incident affecting EGI usage is important.

This is question 26 of the survey

3 REFERENCES

R 1	The EGI Security Policy Group https://wiki.egi.eu/wiki/SPG:Documents
R 2	https://documents.egi.eu/document/83
R 3	https://documents.egi.eu/document/80
R 4	https://documents.egi.eu/public/ShowDocument?docid=771
R 5	https://documents.egi.eu/document/1018
R 6	GOCDB http://goc.egi.eu/
R 7	
R 8	

APPENDIX A – CHECKLIST FORMS

These word tables have been replaced by a choice of the on-line survey at
https://www.surveymonkey.com/s/Cloud_Security_Questionnaire_for_Resource_Centres
Or the editable PDF supplied with this document.