



SMSCG Security Questionnaire

Document info

Document name	SMSCG Security Questionnaire
Document Version	1.2
Identifier	https://cms.smsgg.ch/cms/_WP/WP5/files/Security_Questionnaire.pdf
Date last updated	5/011/09
SMSCG Activity	WP5 Security and Policies

Change history

Version	Date	Author(s)	Comment
1	12/08/09	A. Aeschlimann	Initial after Meeting with au,nw,pf
1.1	24/08/09	P. Flury	Incorporation of SWITCH CERT feedback
1.2	5/11/09	P. Flury	Added question to section 11
1.3	24/11/09	P.Flury	Fix References + comment

Abstract: This document contains security questions that sites contributing with grid resources to the SMSCG need to answer.

Contents

0 Introduction.....	3
0.1 Purpose.....	3
0.2 Procedure and Confidentiality.....	3
1 Scope	3
2 Terms and definitions.....	3
3 (Structure of this document)	3
4 Risk Assessment and treatment	4
4.1 Assessing security risks	4
4.2 Treating security risks.....	4
5 Security Policy	4
5.1 Information Security Policy	4

6 Organization of information security	4
6.1 Internal organization.....	4
6.2 External parties.....	4
7 Asset management.....	5
7.1 Responsibilities for assets.....	5
8 Human resource security	5
9 Physical and environmental security.....	5
10 Communications and operations management	5
11 Access control	5
12 Information System Acquisition, development and maintenance.....	5
13 Information security incident management	6
14 Business continuity management.....	6
15 Compliance	6
References	6

0 Introduction

0.1 Purpose

The purpose of this document is threefold:

1. Assessment: These questions will help to document the status of a site.
2. Prevention of incidents: These questions may help a site to identify weaknesses and to initiate countermeasures (CERT's may already have their guidelines)
3. Procedures for incidents handling may be recommended and aligned with international efforts.

The numbering of the sections in this paragraph closely follows the one of the ISO/IEC27002 document [R1] except when indicated.

0.2 Procedure and Confidentiality

This questionnaire is supposed to be answered by the sites. This must include the CERT people at the sites (definition of „site“ see below). The answers will be treated confidentially.

1 Scope

These questions only regard the facilities involved in the project (but can also be answered for the rest of the Site's infrastructure) see e.g

https://cms.smscg.ch/cms/_WP/WP5/generic_site.html

2 Terms and definitions

Grid Services	A generic resource which is used and shared by the Grid community. Different grid services may have different security requirements.
Local Security Policy	A set of internal security policies as defined by the local legal entity (CERT).
Grid Security Policy	A set of security guidelines for one or more grid services. https://cms.smscg.ch/cms/_WP/WP5/files/Security_Policy.pdf
Site	is a set of services administered by a single group within an institution. (Eg. Chemistry @ UZH, ID@UniBE, LHEP@UniBE...)

3 (Structure of this document)

not relevant

4 Risk Assessment and treatment

4.1 Assessing security risks

Has the site been audited recently by some third party about information security?

4.1.1 Does the site have a security checklist to carry out a security risk assessment?

If yes, has the site done the assessment?

If not why?

4.1.2: Is the site compliant with the SMSCG checklist [R2]?

(If not please give details)

4.2 Treating security risks

4.2.1 Who at the site is making the decision about the security risk treatment?

4.2.2 Are the processes defined and in place? If so please briefly describe them.

5 Security Policy

5.1 Information Security Policy

5.1.1: Has the site implemented a Local Security Policy?

5.1.2: Has the Local Security policy been reviewed lately? What are the site's criteria for a review?

5.1.3: Is the Grid Security Policy already covered by the Local Security Policy?

If not, what changes are necessary?

6 Organization of information security

6.1 Internal organization

6.1.1: Who at the site is in charge of information security and security incidents? (more than one name may be mentioned)

6.1.2: Has the site set up policies controlling the handling of confidential data?

If yes, what are they?

6.1.3: What are the best practices in place referring to information security (brief list)?

6.1.4: Is the Site's information security reviewed independently and periodically?

6.2 External parties

6.2.1: Do you have explicit risk assessment for external parties who have access to the facilities deployed for SMSCG?

6.2.2: Does the site enforce a user policy?

6.2.3: Third party agreements: If present, how are the agreements enforced?

7 Asset management

7.1 Responsibilities for assets

7.1.1 Are your assets (=infrastructure) clearly defined? See assets checklist [R3]. Please do briefly summarize your answer.

8 Human resource security

Since we assume that the sites do have standard procedures eg. for people starting to or leaving work, we do ask only one question here.

8.1.1 Do you have revocation procedures (checklist) when people (staff) leave your institution?

9 Physical and environmental security

9.1 What are the site's current implementations of physical security (eg. physical access)?

10 Communications and operations management

(numbering of the questions in this section is not conform to the numbering of the subsections of the referenced documents)

10.1 Are there any intrusion detection mechanisms implemented? (Please do briefly summarize.)

If yes, who runs them and is responsible for them?

10.2 Are there any procedures implemented for data backup? (Please do briefly summarize)

If yes, who runs them and is responsible for them?

10.3 Who is the network security contact at the site?

10.4 (Monitoring) Does the Site produce audit logs recording user activities, exceptions and information security event and keep them for an agreed amount of time?

If yes, is this information protected against incidents (e.g. dedicated machine for logging)?

11 Access control

(numbering of the questions in this section is not conform to the numbering of the subsections of the referenced documents)

11.1 Is the site part of the AAI federation and does it conform with the policies?

11.2 How do you control access to your Grid services (e.g. standalone UI)? Do you keep Grid services separated (all services on separate machines)?

12 Information System Acquisition, development and maintenance

12.1.1 Does your site have a vulnerability management?

12.1.2 Does your site have a patching management?

13 Information security incident management

(numbering of the questions in this section is not conform to the numbering of the subsections of the referenced documents)

13.1 Is there a specific guide/procedure about what measures should be taken when an incident happens?

13.2 Does the site know who to inform in case of an incident?

13.3 Does the site usually do forensics in case of an incident (e.g. together with the CERT people)?

13.4 Does the site participate in information channels in order to exchange information about incidents with other sites?

14 Business continuity management

(numbering of the questions in this section is not conform to the numbering of the subsections of the referenced documents)

14.1 How much time does it take you to recover „from scratch“ in case of an incident/disaster?

14.2 What recovery procedures have you got in place?

15 Compliance

(numbering of the questions in this section is not conform to the numbering of the subsections of the referenced documents)

15.1 Does the site have guidelines related to legal issues?

15.2 Who is the contact responsible for that?

Glossary

AAI	Authentication and Authorization Infrastructure
AC	Attribute Certificate: Structure similar to a public key certificate with the main difference that it does not contain a public key. See http://www.ietf.org/rfc/rfc3281.txt for details. For the context surrounding AC and VOMS see http://grid-auth.infn.it/docs/AC-RFC.pdf
ARC	Grid middleware stack developed by NorduGrid (see http://www.nordugrid.org)
Attribute	A property of an end entity. In the context of Shibboleth Identity Provider attributes are used to characterize a user.
CA	Certificate Authority: An internal entity or trusted third party that issues, signs, revokes and manages digital certificates.
CE	Computing Element. (Public) front-end to computing resources. Access control and mapping to local resources are performed on this host.
Certificate	Information issued by a trusted party. Used to identify an individual or system.
CERT	Computer Emergency Response Team
Credentials	Evidence asserting the user's right to access certain systems (e.g. username, password, etc)
DN	Distinguished Name: Subject of an X.509 certificate

GIIS	The Grid Index Information Service is a top-level (typically on country level) node that collects and stores information about the Grid. The information is collected from the GRIS'es and uses an own schema.
GRIS	Grid Resource Information Service collects and stores local Grid information (typically of a site). The information from the GRIS/GIIS are used for match-making, i.e. for selecting the suitable resources for jobs upon their submission.
Identity Provider	Authority responsible for generating and asserting authentication, authorization and identity information about their users in a security domain
IGTF	International Grid Trust Federation: Body with the goal to harmonize and synchronize PMAs policies to establish and maintain global trust relationships in e-Science. See http://www.igtf.org for details.
NFS	Network File System
PKI	Public Key Infrastructure: Processes and technologies used to issue and manage digital certificates, enabling third parties to authenticate individual users, services and hosts.
Proxy Certificate (PX509)	A technique to delegate rights from one system to another (remote) system based upon X509 certificates. See http://tools.ietf.org/html/rfc3820 for more details.
SAML	Security Assertion Markup Language: an XML framework for exchanging authentication and authorization information. SAML is a standard of OASIS and is the first standard for federated identity.
Shibboleth	Federated identity management solution from Internet2/MACE (Middleware Architecture Committee for Education). It is the name of the architecture as well as the name of the open source implementation.
Short-lived X.509 certificate	An X.509 certificate with a life time of less than 1 million seconds (approx. 11 days)
SLCS	Short-lived credential service: A service returning a short-lived X.509 certificate to a requester after successful authentication
SWITCHaai	Shibboleth Federation operated within the Swiss higher education and research sector. See http://www.switch.ch/aai for details.
UI	User Interface: host from where the user interacts with the grid software in the gLite middleware environment.
VASH	<u>V</u> oms <u>A</u> tribute from <u>S</u> hibboleth: the name of the Shibboleth Service Provider described in this document. It transfers Shibboleth user attributes into VOMS.
VO	Virtual Organization: arbitrary grouping of people and resources with the goal of conducting a project.
VOMS	Virtual Organization Membership Service: A grid service, which describes and manages the members of a virtual organization.
WN	Worker Node: the entity where jobs get executed.
X.509	ITU-T standard for public key infrastructures. It defines among other things standard formats for certificates. See http://www.ietf.org/rfc/rfc2459.txt for details.
X.509 certificate	Certificate compliant with the format as specified in the X.509 standard.

References

- [R1] ISO/IEC 27002:2005 Information technology – Security techniques – Code of Practice for Information Security Management.
<http://www.iso27001security.com/html/27002.html>
- [R2] Security Risk Assessment Checklist of the SMS CG Project:
https://cms.smsg.ch/cms/_WP/WP5/files/Security_Risk_Assessment_Checklist.pdf
- [R3] Assets Checklist of the SMS CG Project.
https://cms.smsg.ch/cms/_www/admin/assets-checklist.html
- [R4] Layout of a generic SMS CG site (access restricted)
https://cms.smsg.ch/cms/_WP/WP5/generic_site.html