



LCG Grid Operations Service

Procedure for Site Self-Audit



<i>Date:</i>	16 February 2004
<i>Version:</i>	0.2
<i>Status:</i>	Final
<i>Author:</i>	Trevor Daniels



Document Log			
Issue	Date	Author	Comment
0.1	23 Dec 2003	Trevor Daniels	First draft for discussion in GOC Steering Group and LCG Security Group
0.2	16 Feb 2004	Trevor Daniels	Incorporating comments and general tidying up
0.2	8 June 2004	Ian Neilson	Moved to FINAL status following approval by GDB on 18 May 2004



1 Introduction

This document provides guidance to Resource and Service Administrators (hereafter called ‘Resource Administrators’) for meeting the requirements of the LCG Security and Availability Policy and the more detailed documents referenced therein with respect to conducting a Self-Audit of their compliance with that Policy.

The Policy states:

Sites running externally accessible LCG services will be required to conduct a self-audit of their compliance with this Policy, following the Site self-audit Procedure specified by the GOC, at intervals not exceeding 2 years. The GOC will in addition conduct or commission independent audits of compliance on sites failing to meet the requirement for self-audit, on sites appearing to be in breach of this Policy and occasionally on sites selected at random. Statements acknowledging the receipt and summaries (excluding security sensitive information) of both self and independent audits will be published on the GOC website. Such Audits of Compliance will be required for the continued recognition of the service being operated.

This document should be read in conjunction with that Policy.

2 Definitions

LCG is the LHC Computing Grid project which was formed to build the computing environment to support the scientific exploitation of the Large Hadron Collider (LHC) at CERN.

An **LCG Service** is one of the production Grid services which are made available to a remote and general community of LCG users via the Internet. LCG Services include but might not be limited to User Interfaces, Computing Elements, Information Services, Logging and Bookkeeping Services, Resource Brokers, Replica Catalogues, the Security Infrastructure and Storage Elements.

A **Site** is an institute which is providing one or more **LCG Services** to the LHC Computing Grid.

The **LCG Resources** at a site are the hardware, software, data and supporting infrastructure required to provide the LCG Services operated by that site.

The **Resource Administrator** of an LCG Service at a Site is the person responsible for providing and maintaining an LCG Resource or LCG Service at that Site. (Although the singular is used in this document several individuals may actually be involved, including system programmers, operators, user support staff, networking staff and security personnel.)

3 Site Self-Audit

The site self-audit is a check-list, shown at Appendix A, of the main requirements for compliance with the LCG Security and Availability Policy which requests sites to provide simple statements to substantiate their compliance with those requirements.

The procedure for conducting the audit is to access the GOC web page provided for the appropriate site using the credentials of one of the site’s personnel which have been registered for that purpose.

The latest version of each site’s self-audit is displayed on the GOC website, dated and ‘signed’ with the credentials of the person completing the assessment, as the Statement of Compliance section of that site’s Service Level Agreement.



It is recommended that a site renews its self-audit assessment every year. It is a requirement of the Policy that this be done at least every 2 years.

4 Audits Instigated by the GOC

The GOC will conduct or commission independent audits of sites which fail to meet the requirement for self-audit, on sites appearing to be in breach of the Security and Availability Policy and occasionally on sites selected at random. Such independent audits will determine the answers to exactly the same questions as those of the self-audits. The resulting assessments will also be displayed on the GOC web-site, together with the reason for conducting the audit.



A Appendix

To be completed jointly by the Resource Administrators responsible for LCG Services at the named site. Provide single answers to the questions of each section if the answers are identical for all Services, or provide individual answers for each Service if they differ.

A.1 Details of the Site

Name of site:

*A Model Site
E-Science Department*

Services offered.

RB, CE, UI, SE, RC

A.2 Quality of Services

By participating in LCG you have accepted the responsibility to deliver professionally managed and reliable LCG Services.

What actions have you taken to ensure this?

- a) The Resources providing the services are located in a purpose-build, environmentally controlled, secure machine room, managed by professional operators*
- b) All the Services are monitored locally with Nagios for failure with automated 24/7 callout of operational staff*
- c) The SysAdmins are on a call-out roster to provide technical assistance if required*

A.3 Consequent Risks

By participating in LCG you have acknowledged that an increased risk of host compromise may follow and you have accepted the

Model Response

[Note that these are examples of possible answers to the question to indicate the level of detail expected : they should not be taken to indicate a standard that must be attained. Sites should provide answers which reflect their true situation.]



responsibility to minimise that risk by taking local actions.

What actions have you taken to minimise that risk?

- a) *The perimeter firewall has been reconfigured*
- b) *Staff familiar with LCG software are available locally*
- c) *Notices of security alerts and relevant patches are monitored daily and appropriate action is immediately taken*
- d) *Checksums of kernels and other critical components are compared daily to standard values and an alert is raised if anomalies are found*

A.4 Site Policy

By participating in LCG you have accepted the need to ensure that your implementations of LCG Services comply with both your site Security Policy and LCG's Security and Availability Policy.

List any reservations or exceptions, or state there are none.

There are none

A.5 Notifying Site Personnel

By participating in LCG you have accepted the requirement to notify all appropriate personnel concerned with security and system management on your site of the requirements of the LCG Security and Availability Policy.

Who have you notified?

- a) *The site Security Officer*
- b) *Networking staff*
- c) *Operators*
- d) *Line management up to Head of Department*



A.6 Resource Administration

By participating in LCG you have accepted the need to identify Resource Administrators who accept the responsibility for the installation, maintenance and quality of the LCG Services offered by your site.

List the Services offered and the Administrators responsible for each.

*RB: A Whizkid
CE: A Whizkid
UI: B Hacker
SE: B Hacker
RC: B Hacker*

A.7 Service Level Agreement

By participating in LCG you have accepted the requirement to specify and publish SLAs in the prescribed format for each of the services you are offering.

List any Services for which this has not been done, or state that SLAs have been published for all the Services listed under A1.

SLAs have been published for all the Services except the RC, which is not yet operational.

A.8 Physical Security

By participating in LCG you have accepted the requirement to assess the risks to LCG Resources from intruders, fire, flood, power failure, equipment failure and environmental hazards and to reduce them to levels consistent with the service quality specified in the associated SLAs.

List any Services for which this has not been done, or state that the SLAs for all the Services listed under A1 are consistent with your estimates of these risks.

SLAs for all the Services are consistent with the estimates of these risks



If you offer a Certificate Authority service you must meet all the requirements specified in the LCG Procedures for operating and approving such services.

List any exceptions or state that all the requirements are met.

All the requirements are met

A.9 Network Security

By participating in LCG you have accepted the requirement to assess the risks to LCG Resources from intruders and failures of hardware and software and to reduce them to levels consistent with the service quality specified in the associated SLAs.

List any Services for which this has not been done, or state that the SLAs for all the Services listed under A1 are consistent with your estimates of these risks.

SLAs for all the Services are consistent with the estimates of these risks

List the measures which have been taken to provide firewall protection for LCG Resources (in brief outline only).

a) The perimeter firewall is configured to permit incoming connections only to the necessary ports on LCG Resources

List the measures that have been taken to ensure that all critical security-related patches and updates can be applied promptly to all LCG resources.

a) Announcements of security-related patches are reviewed daily

b) A record of the patch status of every host is maintained automatically

c) All SysAdmins are able to patch all Services and they ensure that at least one of them is available every working day

d) SysAdmins are available on call-out if necessary

By participating in LCG you have accepted the requirement to have clearly defined incident response procedures for all LCG Resources.



List the main steps in these procedures.

- a) *Note the open network connections*
- b) *Disconnect the affected system from the network*
- c) *Notify internal CERT team and the LCG Security Officer*
- d) *Run the incident response kit for that system to capture pertinent data and to make checks of critical files*
- e) *Inspect executing processes, open files, etc to gather information about the nature of the compromise and distribute it promptly to colleagues and security officers*
- f) *Take a back-up of the system disk(s) for later investigation*
- g) *Recover the Service by taking whatever steps are required to ensure the intrusion is totally removed*

A.10 Access Control

By participating in LCG you have accepted the requirement to install and maintain the global components of the grid security infrastructures.

What procedures have been implemented to ensure certificates and revocation lists associated with LCG Services and Users are renewed before they expire?

- a) *All revocation lists from all the LCG-recognised CAs are refreshed weekly by a cron job*
- b) *Expiry dates of certificates are monitored by GOC and are renewed when the certificate has less than 4 weeks to live*

A.11 Compliance with Legislation

If there are any areas in the LCG Security and Availability Policy which are in conflict with any local legislation briefly list them and indicate which Services are affected.

There are none