# Accounting Portal Availability and Continuity Plan

## Table of contents



## Introduction

This page reports on the Availability and Continuity Plan for the **Accounting Portal** and it is the result of the risks assessment conducted for this service: a series of risks and treats has been identified and analysed, along with the correspondent countermeasures currently in place. Whenever a countermeasure is not considered satisfactory for either avoiding or reducing the likelihood of the occurrence of a risk, or its impact, it is agreed with the service provider a new treatment for improving the availability and continuity of the service. The process is concluded with an availability and continuity test.

| | Last | Next |
|---|---|---|
| **Risks assessment** | 2022-08 | Q3 2023 |
| **Av/Co plan** | 2022-08 | Q3 2023 |

previous plans are collected here: https://documents.egi.eu/document/3492

## Hardware HA Configuration

- The Accounting Portal service is available in a dedicated virtual machine running in the CESGA cloud framework based on OpenNebula software, which offers high availability thanks to its resources:
  - A pool of physical servers where the virtual machine can run. Over 50 servers with 24 cores and 32GB per server are available. These servers are configured with redundant power supply and two disks in RAID-1 configuration.
  - Storage is provided in a NetApp HA storage solution, providing redundant configuration for data movers (servers) and RAID-TEC (triple parity) protection for the disks; the backup of this storage is performed on a daily basis

## Availability requirements and performances

In the OLA it was agreed the following performances targets, on a monthly basis:

- Availability: 99%
- Reliability 99%

Other availability requirements:

- the service is accessible using SAML which redirects to EGI Check-in.
- the service is accessible via webUI

The service availability is regularly tested by nagios probes (eu.egi.CertValidity and org.nagiosexchange.AccountingPortal-WebCheck): https://argo-mon.egi.eu/nagios/cgi-bin/status.cgi?host=accounting.egi.eu&style=detail

The performances reports in terms of Availability and Reliability are produced by ARGO on an almost real time basis and they are also periodically collected into the Documentation Database.

Over the past years, the Accounting Portal hadn't particular Av/Co issues highlighted by the performances that need to be further investigated.

## Risks assessment and management

For more details, please look at the google spreadsheet. We will report here a summary of the assessment.

## Risks analysis

| Risk id | Risk description | Affected components | Established measures | Risk level | Expected duration of downtime / time for recovery | Comment |
|---|---|---|---|---|---|---|
| 1 | Service unavailable / loss of data due to hardware failure | All | All services are running on virtual machines. In case of hardware failure of the host machine the virtual machine can be re-instantiated in another hypervisor in the private cloud. Daily backups of the service including database data. | Low | In case an instance must be instantiated from backups can take up to two-three working hours. In case latest backups are not available some data must be re-generate from the central accounting repositories and this may take up to two hours. | the measures already in place are considered satisfactory and risk level is acceptable |
| 2 | Service unavailable / loss of data due to software failure | All | Restoring of the codebase via git repository | Low | One to two working hours | the measures already in place are considered satisfactory and risk level is acceptable |
| 3 | service unavailable / loss of data due to human error | All | Restoring of the codebase via git repository, restore of backup of virtual machine, restoring of data from SSM services. | Low | Two to Three working hours. | the measures already in place are considered satisfactory and risk level is acceptable |
| 4 | service unavailable for network failure (Network outage with causes external of the site) | Web frontend | CESGA has redundant network connectivity to the NREN | Low | Close to zero, less than one hour. | the measures already in place are considered satisfactory and risk level is acceptable |
| 5 | Unavailability of key technical and support staff (holidays period, sickness, ...) | All | More personnel have been involved in the operation of the Accounting portal, this ensures actions taken within the OLA goals every working day. There is also internal documentation with management procedures and portal architecture. | Low | Within the OLA targets for operational actions Longer periods in case of bugs or maintenance (one week) because not all the personnel can develop patches to the code. | the measures already in place are considered satisfactory and risk level is acceptable |
| 6 | Major disruption in the data centre. Fire, flood or electric failure for example | All | The computing centre has electric backup system and fire control devices. In case of an occurrence despite the controls, the virtual machine can be instantiated elsewhere. | Medium | 1-2 weeks, the time to deploy recover operational status at CESGA or the service to another resource centre partner of the NGI | the measures already in place are considered satisfactory and risk level is acceptable |
| 7 | Major security incident. The system is compromised by external attackers and needs to be reinstalled and restored. | Frontend and DB | Daily backup are executed. Backup is stored in a separate system and can be restored in another VM | Low | 1-2 work hours. In case new host certificates are required, up to 2 days. | the measures already in place are considered satisfactory and risk level is acceptable |
| 8 | (D)DOS attack. The service is unavailable because of a coordinated DDOS. | Web interface | NREN provides protection for DOS attacks, firewall can limit impact of the DDoS | Low | Depending on the attack, few hours maximum | the measures already in place are considered satisfactory and risk level is acceptable |

## Outcome

The level of all the identified risks is acceptable and the countermeasures already adopted are considered satisfactory

## Additional information

The provider has straightforward and semi-automatic procedures to invoke as countermeasure in case of risk occurrence (in particular for risks 1,2,3,5, and 7)

The Availability targets don't change in case the plan is invoked.

Recovery requirements:

- **Maximum tolerable period of disruption (MTPoD)** (the maximum amount of time that a service can be unavailable or undelivered after an event that causes disruption to operations, before its stakeholders perceive unacceptable consequences): 1 week
- **Recovery time objective (RTO)** (the acceptable amount of time to restore the service in order to avoid unacceptable consequences associated with a break in continuity (this has to be less than MTPoD)): 5 days
- **Recovery point objective (RPO)** (the acceptable latency of data that will not be recovered): n.a. (data can be republished)

Approach for the return to normal working conditions as reported in the risk assessment.

The support unit **Accounting Portal** shall be used to report any incident or service request

The providers can contact EGI Operations via ticket or email in case the continuity plan is invoked, or to discuss any change to it.

# Availability and Continuity test

The proposed A/C test will focus on a recovery scenario: the service is supposed to have been disrupted and needs to be reinstalled from scratch. Typically this covers the risks 1,2, and 7. The last backup of the data will be used for restoring the service, verifying how much information will be lost, and the time spent will be measured.

Performing this test will be useful to spot any issue in the recovery procedures of the service.

The test hereby described was done on 2nd August 2021 and a scheduled downtime was announced.

## Test details

The production machine has been turned off and a new one created; the last backup data have been used to restore the system. The recovery, starting from the instantiation of the new machine and including the testing of the portal functionality, took less than 2 hours.

## Test outcome

The test can be considered successful: the service can be restored in few time and there are no loss of data. Even if the service is not available for few hours or a day, this can be considered acceptable: the portal is used for displaying and collecting accounting information, the other infrastructure services are not depending on it. Only infrastructure/operations centres/resource centres/VOs managers would suffer of a temporary disruption of the service.

# Revision History

| Version | Authors | Date | Comments |
|---|---|---|---|
| | Alessandro Paolini | 2018-05-03 | first draft, discussing with the provider |
| | Ivan Diaz, Alessandro Paolini | 2018-05-28 | added a paragraph about HA configuration; added information about the test |
| | Alessandro Paolini | 2018-08-15 | added the paragraph Test Outcome, plan finalised |
| | Alessandro Paolini | 2019-08-19 | starting the yearly review.... |
| | Alessandro Paolini | 2019-09-10 | recovery test performed, information update, plan finalised. |
| | Alessandro Paolini, Ivan Diaz | 2020-12-09 | yearly review completed, updated the availability requirements; agreed to perform a new recovery test on March /April 2021 |
| | Alessandro Paolini | 2021-08-04 | new recovery test performed, updated the related section |
| v. 6 | Alessandro Paolini | 2022-08-12 | yearly review; updated risk number 6; no need to repeat the recovery test. |