EUROPEAN MIDDLEWARE INITIATIVE

SOFTWARE MAINTENANCE QUALITY CONTROL REPORT

EU DELIVERABLE: D3.3.1

Document identifier:	**EMI-D3.3.1-Software_Maintenance_Quality_Control_Report-v1.5.odt**
Date:	**19/11/2010**
Activity:	**SA1.4**
Lead Partner:	**CINECA**
Document status:	**Version 1.5**
Document link:	

Abstract:
This document describes the status and performance of the quality control task which details with the availability and execution of regression tests for the supported EMI components, test unit availability and coverage and various static and dynamic metrics on released components.

Copyright notice:

Copyright (c) Members of the EMI Collaboration. 2010.

See http://www.eu-emi.eu/about/Partners/ for details on the copyright holders.

EMI ("European Middleware Initiative") is a project partially funded by the European Commission. For more information on the project, its partners and contributors please see http://www.eu-emi.eu.

This document is released under the Open Access license. You are permitted to copy and distribute verbatim copies of this document containing this copyright notice, but modifying this document is not allowed. You are permitted to copy this document in whole or in part into other documents if you attach the following reference to the copied elements: "Copyright (C) 2010. Members of the EMI Collaboration. http://www.eu-emi.eu ".

The information contained in this document represents the views of EMI as of the date they are published. EMI does not guarantee that any information contained herein is error-free, or up to date.

EMI MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, BY PUBLISHING THIS DOCUMENT.

Delivery Slip

	Name	Partner / Activity	Date	Signature
From	Giuseppe Fiameni	CINECA/SA1.4	09/24/2010	
Reviewed by	Maria Alandes Pradillo/Shiraz Memon			
Approved by				

Document Log

Issue	Date	Comment	Author / Partner
1	09/24/2010	First draft	Giuseppe Fiameni/CINECA
2	10/21/2010	First release	Giuseppe Fiameni/CINECA
3	10/26/2010	Release 1.4	Giuseppe Fiameni/CINECA
4	17/11/10	Release 1.5 *Changes according to official reviews*	Giuseppe Fiameni/CINECA

Document Change Record

Issue	Item	Reason for Change
1		
2		
3		

TABLE OF CONTENTS

Table of Contents

1. INTRODUCTION

1.1. PURPOSE

Quality Control (QC) verifies the application of Quality Assurance (QA) processes and procedures and, through the execution of periodic reviews, reports and measures the status and performance of the SA1 work respectively. This Quality Control report is meant to provide an aggregated view of quality inspection results and performance measurements, and to highlight which changes are necessary to correct anomaly or nonconformity discovered during the control process. The change requests are submitted to the QA that, on the base of project's priorities, determines which can be approved and then applied, which require further evaluations and which are simply discarded.

1.2. DOCUMENT ORGANIZATION

The document is organized as follows:

- Chapter 1 and 2 are the Introduction and the Executive Summary respectively;
- Chapter 3 presents the organization of the Quality Control activity and the interaction with the Quality Assurance;
- Chapter 4 reports the results of the Quality Review scheduled for PM6;
- Chapter 5 describes the status of the Regression Tests;
- Chapter 6 reports the conclusions of the work.

1.3. REFERENCES

R1	**Quality Assurance Plan**, *https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDSA21*
R2	**Quality Assurance Metrics**, *https://twiki.cern.ch/twiki/bin/view/EMI/TSA23*
R3	**Quality Assurance Wiki Page**, *https://twiki.cern.ch/twiki/bin/view/EMI/SQAP*
R4	**Software Release Schedule**,
R5	**Software Release Plan**, *https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDSA12*
R6	**Software Maintenance and Support Plan**, *https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDSA11*
R7	**Technical Development Plan**, *https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDNA131*
R8	**Release Management Wiki Page**, *https://twiki.cern.ch/twiki/bin/view/EMI/TSA13*
R9	**Configuration and Integration guidelines**, *https://twiki.cern.ch/twiki/bin/view/EMI/EmiSa2ConfigurationIntegrationGuidelines*
R10	**Certification and testing guidelines,**

	https://twiki.cern.ch/twiki/bin/view/EMI/EmiSa2CertTestGuidelines
R11	**Change management guidelines**, *https://twiki.cern.ch/twiki/bin/view/EMI/EmiSa2ChangeManagementGuidelines*
R12	**DSA2.2.1 - QA Tools Documentation**, *https://twiki.cern.ch/twiki/bin/edit/EMI/DeliverableDSA221?topicparent=EMI.EmiDeliverables;nowysiwyg=1*
R13	**Certification report Template**, *https://twiki.cern.ch/twiki/bin/edit/EMI/EMICertificationReportTemplate*
R14	**Software Verification and Validation Template**, *https://twiki.cern.ch/twiki/bin/view/EMI/SoftwareVerAndValTemplate*
R15	**Quality Control Report PM6**, *https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCPM6*
R16	**Software Quality Assurance Plan Documentation**, *https://twiki.cern.ch/twiki/bin/view/EMI/SQAP#SQAP_Documentation*
R17	**Firs Principles Vulnerability Assessment**, *http://www.cs.wisc.edu/mist/VA.pdf*
R18	**Review of the Software Release Plan**, *https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCRSRP*
R19	**Review of the Software Release Schedule,** *https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCRSRS*
R20	**Review of the Software Maintenance and Support Plan,** *https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCRSMSP*
R21	**Review of the Security Assessments**, *https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCRSA*
R22	**Consejo Superior de Investigaciones Cientificas**, *http://www.csic.es*
R23	***First principles vulnerability assessment,*** *Proceedings of the 2010 ACM workshop on Cloud computing security workshop, James A. Kupsch, Barton P. Miller, Elisa Heymann, Eduardo César*

1.4. DOCUMENT AMENDMENT PROCEDURE

This document can be amended by the authors further to any feedback from other teams or people. Minor changes, such as spelling corrections, content formatting or minor text re-organisation not affecting the content and meaning of the document can be applied by the authors without peer review. Other changes must be submitted to peer review and to the EMI PEB for approval.

When the document is modified for any reason, its version number shall be incremented accordingly. The document version number shall follow the standard EMI conventions for document versioning.

The document shall be maintained in the CERN CDS repository and be made accessible through the OpenAIRE portal.

1.5. TERMINOLOGY

ABI	Application Binary Interface
API	Application Programming Interface
CDS	CERN Document Server
CSIC	Consejo Superior de Investigaciones Cientificas
DCI	Distributed Computing Infrastructure
DMSU	Deployed Middleware Support Unit
EGI	European Grid Infrastructure
EMT	Engineering Management Team
ETICS	eInfrastructure for Testing, Integration and Configuration of Software
FPVA	First Principles Vulnerability Assessment
GGUS	Global Grid User Support
ITIL	IT Infrastructure Library
KPI	Key Performance Indicator
kSLOC	Kilo Source Lines Of Code
MCB	Middleware Coordination Board
NGI	National Grid Initiative
PEB	Project Executive Board
PTB	Project Technical Board
QA	Quality Assurance
QC	Quality Control
RfC	Request for Change
SLA	Service Level Agreement
SQAP	Software Quality Assurance Plan
SU	Support Unit

2. EXECUTIVE SUMMARY

Performing Quality Control is an activity specifically concerned with the monitoring of work results to see whether they comply with the quality standards set out in the SQAP (Software Quality Assurance Plan) defined in SA2 [R1]. Operating throughout the project, its aim is to identify unacceptable or non-conformable results and to inform the QA (Quality Assurance) about their existence so that corrective actions can be undertaken to eliminate, or mitigate, negative impacts on project's outcomes. Basically, all EMI components need to satisfy well-defined quality standards before being included in a stable EMI distribution. The adoption of quality standards must be sufficient to guarantee, to a high degree of confidence, that all EMI materials (software components, documentation, etcetera) meet the requirements, in term of quality parameters, set by EMI customers.

The QC in SA1 is responsible to carry out the following two major activities

- **perform periodic reviews** that**,** scheduled every three months, aim to constantly control the performance of the team and collect measurements for evaluating quality metrics with the use of control tools, such as check lists, control lists and metrics set out in the SQAP. Further information about the scheduled quality reviews can be found at [R15];
- **elaborate project deliverables** to summarize and further investigate the results of periodic reviews with the objective to point out any non-conformity or deviation from quality standards that might became defects in the future.

Besides the execution of quality controls, the QC task also deals with two further activities: a) the security assessment of EMI components; b) the verification that no regression is introduced in software code when changes are applied.

The goal of the Security Assessment activity, which is carried on with the collaboration of CSIC (*Consejo Superior de Investigaciones Cientificas*) [R21], is to ensure and verify that security controls and best practises are introduced and respected during the design and implementation of EMI components. The SQAP requires the creation of a specific plan to describe how the assessment is conducted and, to enforce the importance of developing secure code, defines a quality review to control that all the analysis set in the plan have been carried out and that any critical vulnerability or security problem reported to developers. The plan, which has not been released yet, will found its basis on the FPVA approach (First Principles Vulnerability Assessment) [R22]. FPVA allows to evaluate the security of a system in depth and has shown to be effective in several real systems, finding many serious vulnerabilities. Many of these vulnerabilities reflect common serious mistakes made in distributed services, such as Grid Middlewares. These mistakes include erroneous or changeable configuration files, injection attacks and race conditions. Although the security assessment plan has not been released yet, the assessment of some EMI components (i.e. Argus and gLExec) is already in progress and preliminary results will be delivered soon.

It the following the outcomes of quality controls performed at PM6 are reported, including the results of quality checks, the list of quality nonconformities arose during the control process and the changes requested to QA to help improving the quality of the project.

Before delving into details, it is important to underline that at the time of writing (PM6) since no official EMI releases have been released yet, it has been impossible to collect and perform real

measurements and checks. Nevertheless, the quality controls have been executed anyway and where possible, real values collected and analysed. The nonconformities and the change requests reported in the following paragraphs are intended to be effective and for each of them a response, according to the change management procedure defined in the SQAP, is expected. The change requests, either corrective or preventive, can contribute to the improvement of project quality and should be recorded in the project's documentation to ensure their traceability.

3. THE ORGANIZATION OF THE QUALITY CONTROL

The diagram below (Figure 1) describes how the QC and the QA interact and in which way the information flows between them.

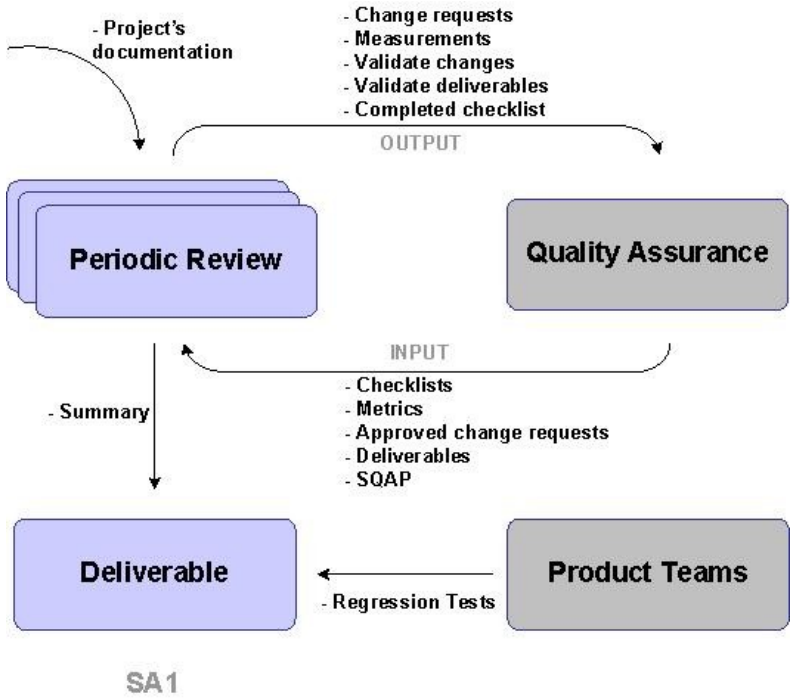


Figure 1: Quality Control Information flow

3.1. INPUTS

This paragraph presents the list of the information items that the QC receives as input and that are fundamental for the execution of reviews.

Quality Assurance Plan

The SQAP specifies the procedures, the metrics and the manner in which the EMI project is to achieve its quality goals in terms of software development.

Quality Checklists

A check-list is a structured tool used to verify whether the required steps in a process have been met. As each step is completed, it is checked off the list. In accordance to the SQAP, the input checklists for the QC in SA1 are:

- Review of the Software Release Plan
- Review the Software Release Schedule
- Review the Software Maintenance and Support Plan
- Security Assessments

Quality Metrics

A quality metric is an operational definition that describes, in very specific terms, a project or product attribute and how the QC process will measure it.

The metrics defined for the QC in SA1 are:

- Review of the Software Release Plan
  - *No metric defined for this review*
- Review the Software Release Schedule
  - *Delay on the release schedule (ID: DELAYONTHERELEASE)*
- Review the Software Maintenance and Support Plan
  - *Total user incidents per user month (ID: TOTALUSERINCIDENTS)*
  - *Training and support incident per user month. (ID: TRAININGSUPPORTINCIDENTS)*
  - *Average time to deal with an incident at the 3rd level of user support (ID: AVERAGETIMEFORUSERINCIDENTS)*
- Security Assessments
  - *No metric defined for this review*

Approved change requests

An approved change request refers to a change request that has been submitted by the QC during a previous review, has been reviewed by the QA and has been authorized to be applied. The list of approved change requests is provided as input to verify that their implementation is correct and satisfies the quality standards Approved change requests can include modifications to the work methods or to the schedule and come as a result of the change management process led by the PEB.

Currently, there are no previous approved changes that need to be verified.

Deliverables

This is the list of deliverables (i.e. documents, products) that the QC verifies

3.2. OUTPUTS

This paragraph presents the list of the information items that the QC returns to the QA for further elaboration.

Change Requests

This is the list of recommended corrective or preventive actions for preventing future defects in procedures or products.

Measurements

Quality control measurements are the documented results for the associated metrics.

Validated changes

Validated changes are results of approved changes, defect repairs, or variances that have been inspected and corrected. Any changed or repaired procedures or products are once again verified and will be either accepted or rejected before the final decision is provided.

Validated deliverable

Validated deliverables are the verified deliverables which have been through the QC process. A deliverables is a verifiable product or service that are produced and provided by the project work.

Completed checklists

Completed checklists are output of the QC activity and become part of the project's documentation.

4. QUALITY CONTROL REVIEW

According to the schedule defined in the SQAP, this QC review refers to PM6 and it is the first performed within the SA1. In the following, the outcomes for each planned review are presented, including the information received as input and that returned as output.

4.1. REVIEW OF THE SOFTWARE RELEASE PLAN

The aim of the *Review of the Software Release Plan* [R18] is to check that the software release plan is up to date and that it fully describes the actual release process.

At the time of writing, the Software Release Plan has not been released yet. Its unavailability has caused all the related checks to fail culminating in a non-conformity problem.

4.1.1 Input

Checklists

- *Checklist for the Review of the Software Release Plan [R18] .*

Metrics

- *No metrics defined for this review.*

Approved change requests

- *No previous approved changes defined for this review.*

Deliverables

- *Software Release Plan [R5].*

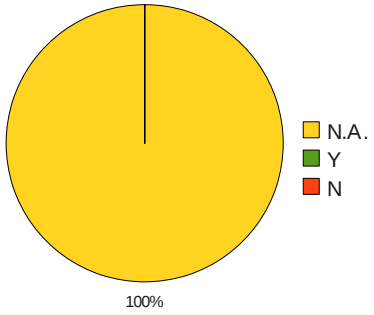
4.1.2 Output

Completed Checklist

Check Number	Question	Re-sponse
1	Does the list of supported platforms correspond to the actual set of platforms on which software components are released?	N.A.
	see Software Release Plan [R5]	
2	Is the installation of external dependencies well documented?	N.A.
	see Software Release Plan [R5]	
3	Are instructions to build the software up to date?	N.A.
	see Software Release Plan [R5]	
4	Is the list of supported delivery software formats up to date (source and binary packages, tarball, package lists, etc)?	N.A.
	see Software Release Plan [R5]	

5	Is the description of the process on how to handle changes up to date?	N.A.
	see Software Release Plan [R5]	
6	Are the communication channels published with updated information?	N.A.
	see Software Release Plan [R5]	
7	Is the process on how to deliver software to the Production Infrastructures up to date and it's aligned to what the Production Infrastructures are expecting?	N.A.
	see Software Release Plan [R5]	

Table 1: Review of the Software Release Plan (N.A. = Not Available)



- 100% of the checks returned N.A. (The N.A. response means that the check cannot be performed either for the unavailability of input information or the inapplicability of the check)

Measurements

There are no measurements defined for this review.

Comments

The table below (Table 2) reports specific comments for the checks that have returned a non-satisfactory response (i.e. N.A. or N). It strongly recommended to take all the comments in account and to take corrective actions in response to the change requests defined for this review.

Check Number	Comments
1	Does the list of supported platforms correspond to the actual set of platforms on which software components are released?
	The information to perform the check is not available.
2	Is the installation of external dependencies well documented?
	The information to perform the check is not available. *In addition, whether the check is referring to the installation of external dependencies in ETICS or to the installation of external dependencies for the deploy of the EMI components, no documentation is available in both cases.*

3	Are instructions to build the software up to date?
	The information to perform the check is not available.
4	Is the list of supported delivery software formats up to date (source and binary packages, tarball, package lists, etc)?
	The information to perform the check is not available.
5	Is the description of the process on how to handle changes up to date?
	The information to perform the check is not available.
6	Are the communication channels published with updated information?
	The information to perform the check is not available.
7	Is the process on how to deliver software to the Production Infrastructures up to date and it's aligned to what the Production Infrastructures are expecting?
	The information to perform the check is not available.

Table 2: Review of the Software Release Plan – Comments

Validated changes

There are no previous change requests that require to be validated for this review.

Validated Deliverables

Name of the deliverable under evaluation	Validated	
	YES	NO
Software Release Plan		X

The Software Release Plan cannot be validated since the related document is not available.

Variations from previous report

There are no variations from the previous review that can be reported here. The variations analysis will be performed starting from the next review when more information on review outcomes will be available.

Change requests

The changes suggested/requested for this report are:

- ***speed-up*** *the completion of the Software Release Plan;*
- ***define*** *the tolerance range of positive checks considering the deliverable validated. It is not clear how many positive checks are needed to consider the Software Release Plan validated.*

The possibility of submitting change requests to the checklist structure (e.g. question text, number of questions, etcetera) will be considered later on during the project when more information on the effectiveness of the review checks should be available.

4.2. REVIEW THE SOFTWARE RELEASE SCHEDULE

The *Review of the Software Release Schedule* [R19] checks that the priorities of the project are taken into account and reflected in the scheduled releases.

The *Software Release Schedule* [R15] is a document requested by the SQAP. At the time of writing, it has not been released yet. Due to its unavailability all the related checks have failed leading to a non-conformity problem.

4.2.1 Preamble on the EMI-0 release

According to the DoW, the first EMI release (EMI-1) will be delivered in March 2011. The product teams are currently working on an "exercise" release designed to understand how to apply the agreed procedures, finding any problem about tools and processes and in general fine tune the EMI software engineering process before the EMI-1 release. The outcome of this exercise release, called EMI-0, is not expected to be made available to external users. Its main goal is to prepare a consistent, coherent repository of non-conflicting packages by the end of October 2010 without any specific commitment on functionality. For further information about the status of the EMI-0 release, please refer to [R7].

4.2.2 Input

Checklists

- *Checklist for the Review of the Software Release Schedule [R19].*

Metrics

- *Delay on the release schedule (ID: DELAYONTHERELEASE).*

Approved change requests

- *No previous approved changes defined for this review.*

Deliverables

- *Software Release Schedule [R15].*

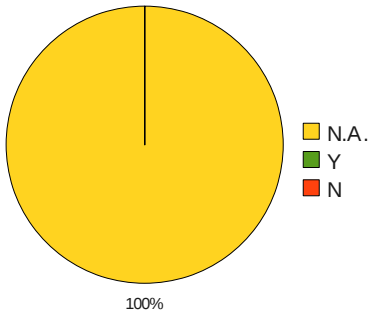
4.2.3 Output

Completed Checklist

Check Number	Question	Response
1	*Has the previous schedule been kept?*	N.A.
	see Software Release Schedule [R1]	

2	*Does the new schedule take into account what wasn't accomplished in the previous schedule?*	N.A.
	see Software Release Schedule [R1]	
3	*Is the r chedule aligned to the Software Development Plan and the priorities of the project?*	N.A.
	see Software Release Schedule [R1]	

Table 3: Review the Software Release Schedule



- 100% of the checks returned N.A. (The N.A. response means that the check cannot be performed either for the unavailability of input information or the inapplicability of the check)

Measurements

In the following, the metrics list defined for this review is reported.

ID	DELAYONTHERELEASE
Name	Delay on the release schedule
Description	This metric could be provided as a histogram showing the delay time (in days) for each release, weighted using the release time
Unit	(release delay)/(release time) * 100
Measurement	**Approximately 20 days**
Thresholds/target value	Ideally the release deadlines should be always met, leading to 0 delays for each release. Proper thresholds have to be defined. The trend of the delays over time could provide useful hints for process optimization.
Comment	According to the EMI DoW, the first EMI release will be made available at the end of March 2011 and thus no measurements can be collected for this metric. However, a preliminary release, called EMI-0, has be scheduled for the end of October 2010 but at the time of writing it has not been released yet leading to a delay of **approximately 20 days.** However, the metric definition should be revisited since it is not clear how the delay should be reported.

Table 4: Delay on the release schedule – Metric

Comments

The table below reports specific comments on the check results.

Check Number	Comments
1	*Has the previous schedule been kept?*
	Since the Software Release Schedule has not been released yet, this check cannot be performed. The information that is necessary to make the comparison is not available.
2	*Does the new schedule take into account what wasn't accomplished in the previous schedule?*
	Since the Software Release Schedule has not been released yet, this check cannot be performed. However, it is not clear how changes or modifications across different releases are tracked. For instance it is not clear how to verify that what was not accomplished in previous releases has been included in the release under review. The adoption of a change tracking system is strongly encouraged.
3	*Is the new schedule aligned to the Software Development Plan and the priorities of the project?*
	Since the Software Release Schedule has not been released yet, this check cannot be performed. Although it is out of scope of this review, it is useful to report that in the Technical Development Plan [R6] and in the various its sub plans, there is no evidence of the development road-map. GANTT charts or progress tables will certainly help the Quality Control activity in elaborating more accurate review. At the moment only sparse pieces of information, scattered among various paragraphs, are available. In some cases the reported information is too vague (i.e. expression like "during the first year") making the execution of check difficult to perform. Moreover, even when deadlines are mentioned, there is no reference to any official document that might consent the QC to verify that those deadlines are met or not.

Table 5: Review the Software Release Schedule - Comment

Validated changes

There are no previous change requests that require to be validated for this review.

Validated Deliverables

Name of the deliverable under evaluation	Validated	
	YES	NO
Software Release Schedule		X

The Software Release Schedule cannot be validated since the related document is not available.

Variations from previous review

There are no variations to report from the previous review.

Change requests

The changes suggested/requested for this report are:

- ***speed-up*** *the completion of the Software Release Schedule;*
- ***define*** *the tolerance range of positive checks considering the deliverable validated. It is not clear how many positive checks are needed to consider the Software Release Plan validated.*

4.3. REVIEW THE SOFTWARE MAINTENANCE AND SUPPORT PLAN

The Review of the Software Maintenance and Support Plan [R19] checks that the plan is up to date and describes the actual maintenance and support processes and that the SLAs are respected.

The Software Maintenance and Support Plan is accessible at [R5].

4.3.1 Input

Checklists

- *Checklist for the Review the Software Maintenance and Support Plan [R19].*

Metrics

- *Total user incidents per user month (ID: TOTALUSERINCIDENTS)*
- *Training and support incident per user month. (ID: TRAININGSUPPORTINCIDENTS)*
- *Average time to deal with an incident at the 3rd level of user support (ID: AVERAGETIMEFORUSERINCIDENTS)*

Approved change requests

- *No previous approved changes defined for this review.*

Deliverables

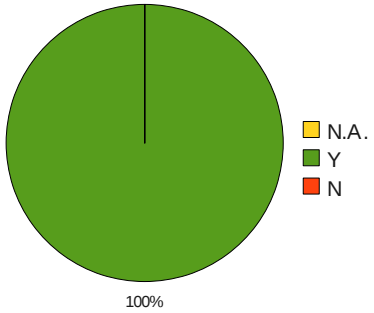
- *Software Maintenance and Support Plan [R5]*

Completed Checklist

Check Number	Question	Re-sponse
1	*Is the process on how to handle incidents reported by EMI users using GGUS up to date?*	Y
	see Software Maintenance and Support Plan [R5]	
2	*Is the process on how to handle requests coming from EMI users or other PTs up to date?*	Y
	see Software Maintenance and Support Plan [R5]	
3	*Is the process on how to handle problems up to date?*	Y

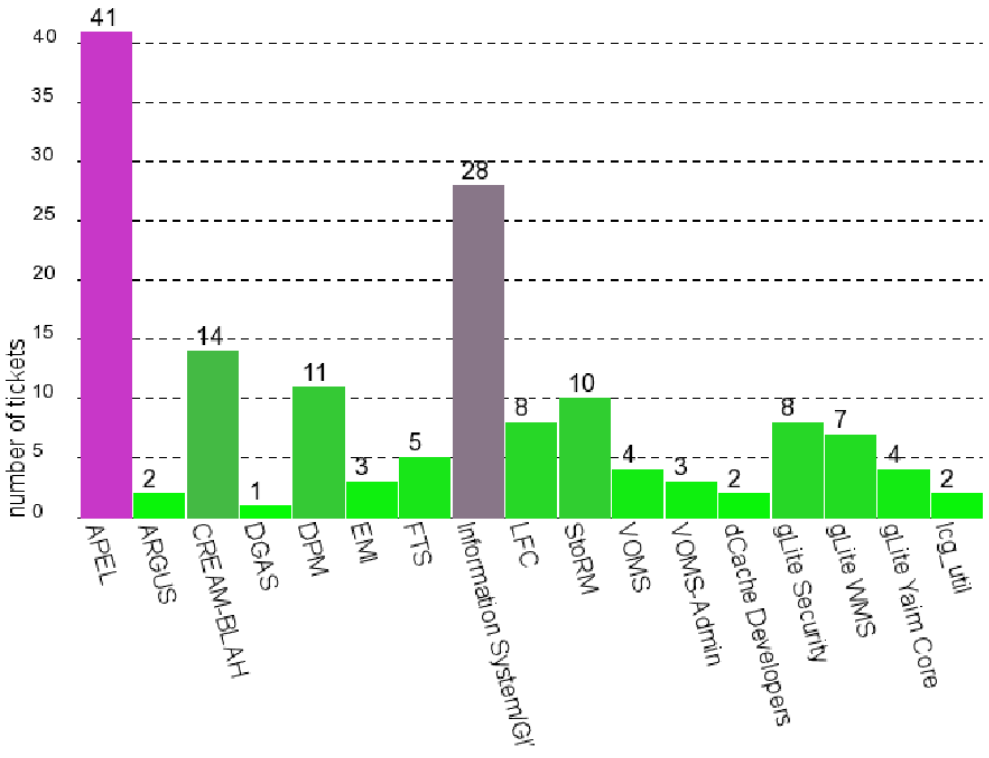
	see Software Maintenance and Support Plan [R5]	

Table 6: Review the Software Maintenance and Support Plan



- 100% of the checks returned Y

Measurements

ID	TOTALUSERINCIDENTS
Name	Total user incidents per user month
Description	This metric covers defects not only in the software but also in the documentation, training and user support processes, per user month. User month means the number of users (in our case, deployed services?) per month.
Unit	GGUS tickets per user per month
Measurement	

	The chart reports the number of incidents submitted during the first six months of project activity.
Thresholds/target value	It is difficult to state a threshold valid for all the product teams, in general a decreasing trend would show positive results.
Comment	The measurement collected for this metric reports the number of incidents submitted to GGUS for all EMI Support Units from May 2010 to October 2010.

Table 7: Total user incidents per user month

ID	TRAININGSUPPORTINCIDENTS
Name	Training and support incident per user month.
Description	This metric covers defects in the training and user support processes, per user month. User month means the number of users (deployed services?) per month. The training and support defects can be derived by subtracting the tickets in status unsolved (ticket that generated a bug) from the total number of opened tickets. It relies on proper bug opening from GGUS tickets, especially for what concerns ambiguous or missing documentation.
Unit	Incident per user month
Measurement	N/A
Thresholds/target value	Decreasing trend.
Comment	At the moment this metric definition has to be updated cause there not exists a ticket category to specify training and support incidents. New development in GGUS is required to calculate this metric.

Table 8: Training and support incident per user month – Metric

ID	AVERAGETIMEFORUSERINCIDENTS
Name	Average time to deal with an incident at the 3rd level of user support
Description	This metric wants to measure the effectiveness of a product team to provide 3rd level user support. The time is measured from the time the ticket reaches a PT's 3rd level support and the time the ticket is moved to the status solved or unsolved
Unit	Days

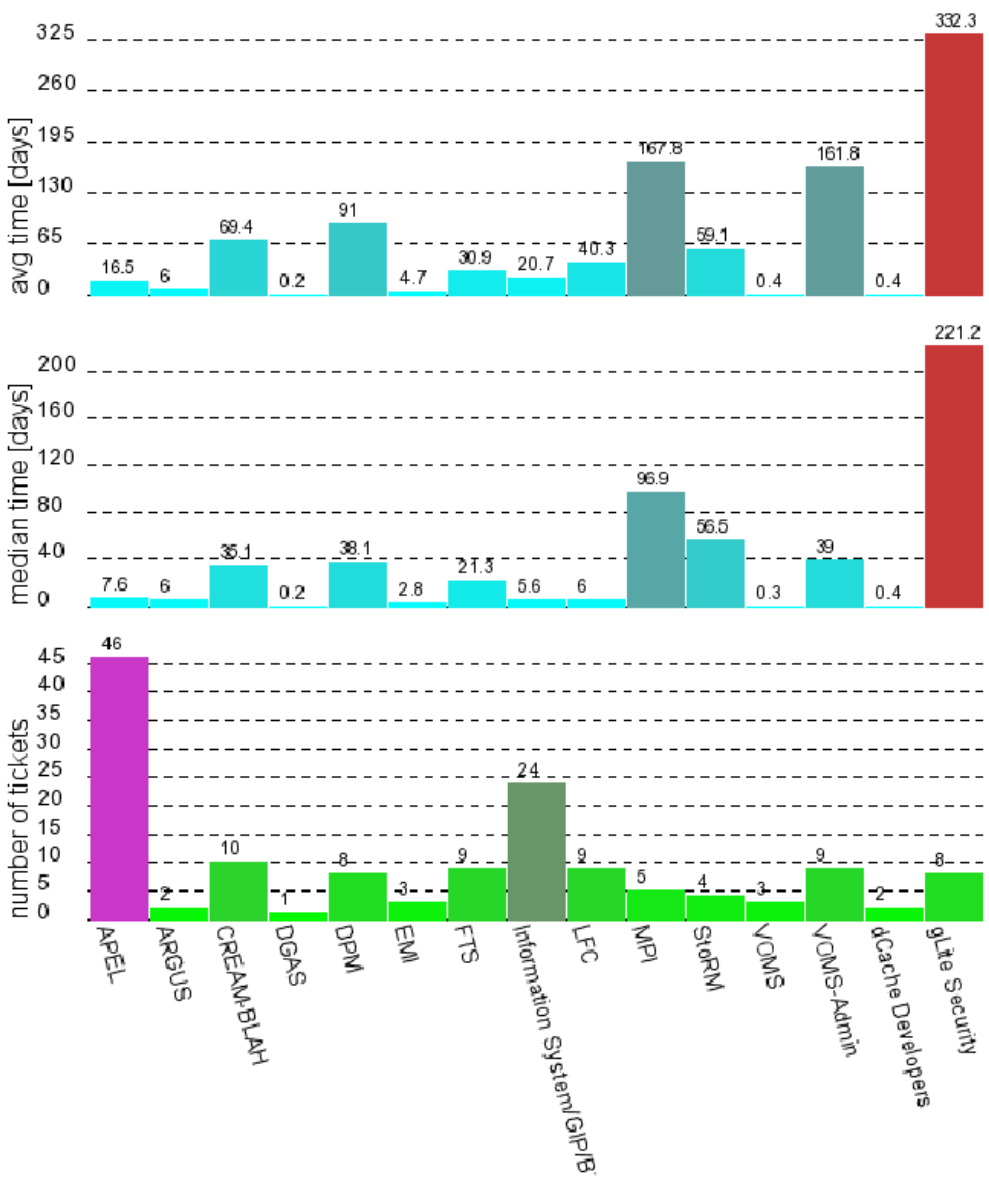
Measurement	 The chart reports the number of incidents submitted for each EMI Support Unit and the time, in days, spent to resolve each of them.
Thresholds/target value	Need project wide agreement.
Comment	The measurement collected for this metric reports the number of incidents submitted to GGUS for each EMI Support Unit from May 2010 to October 2010 and the time spent to solve each of them.

Table 9:Average time to deal with an incident at the 3rd level of user support - Metric

Comments

The outcome of this report partly complies with the quality standards set out for the Software Maintenance and Support plan. Real measurements for the quality metrics were collected and the

outcomes are available in table. Some adjustments to the GGUS interface are still under development especially for calculating the training and support incidents per user month.

Besides the comments reported above, it is important to report that there exists an overlap in quality indicators definition that needs to be addressed to avoid conflicts or reworks. The quality metrics set out for this review and the KPIs [R5] (namely **KSA1.1 and KSA1.2**) defined at the project level might potentially generate the same results leading to overlaps or crossings . To reduce the risk of conflicts, the definition of the two indicators should be revised according to project's priorities and the task for the evaluation of their results concentrated in one single control.

Validated changes

There are no previous change requests that require to be verified for this review.

Validated Deliverables

Name of the deliverable under evaluation	Validated	
	YES	NO
Software Maintenance and Support Plan	Y	

Variations from the previous review

There are no variations to report from the previous review.

Change requests

The changes suggested/requested for this review are:

- ***define*** *the tolerance range of positive checks considering the deliverable validated. It is not clear how many positive checks are needed to consider the Software Maintenance and Support Plan validated;*
- ***define*** *the metric thresholds for considering the deliverable validated;*
- ***consider*** *to aggregate the quality metrics defined for this review with the project KPIs (KSA1.1 and KSA1.2).*

4.4. SECURITY ASSESSMENTS

The Review of the Security Assessment should check that the different stages described in the First Principles Vulnerability Assessment (FPVA) approach are being followed. FPVA is a primarily analyst-centric (manual) approach to assessment whose aim is to focus the analyst's attention on the parts of the software system and its resources that are mostly likely to contain vulnerabilities. FPVA is designed to find new threats to a system. It's not dependent on a list of known threats.

At the time of this quality control, the Security Assessment Plan has not been completed and released yet. Its unavailability has caused all related quality checks defined for it to fail culminating in the issuing of a non-conformity problem. Nevertheless the assessment of some EMI components (i.e. Argus and gLExec) has already started and the first outcomes are expected to be released in the next weeks.

4.4.1 Input

Quality Checklists

- *Checklist for the Review of the Security Assessment [R20].*

Quality Metrics

- *No metrics defined for this review.*

Approved change requests

- *No previous approved changes defined for this review.*

Deliverables

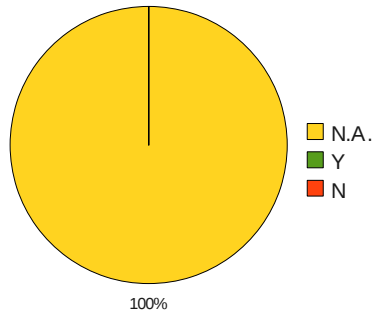
- *Security Assessment Plan [R15].*

4.4.2 Output

Completed Checklist

Check Number	Question	Response
1	The Architectural Analysis has been carried out and the output contains a diagram describing the interactions among components and end users.	N.A.
2	The Resource Identification has been carried out and the output contains the resource descriptions.	N.A.
3	The Trust and Privilege Analysis has been carried out and the output contains the trust levels and the delegation information for all the components and their interactions.	N.A.
4	The Component Evaluation has been carried out and the output contains identified vulnerabilities and their suggested fixes.	N.A.
5	The Dissemination of Results has been carried out.	N.A.

Table 10: Review of the Security Assessment Plan (N.A. = Not Available)



- 100% of the checks returned N.A. (The N.A. response means that the check cannot be performed either for the unavailability of input information or the inapplicability of the check)

Measurements

There are no measurements for this review.

Validated changes

There are no previous change requests that require to be verified for this review.

Validated Deliverables

Name of the deliverable under evaluation	Validated	
	YES	NO
Security Assessment Plan		X

The Security Assessment Plan cannot be validated since the related document is not available.

Variations from previous report

There are no variations from the previous review to report.

Change requests

The changes suggested/requested for this review are:

- ***speed-up*** *the completion of the Security Assessment Plan;*
- ***define*** *the tolerance range of positive checks considering the deliverable validated. It is not clear how many positive checks are needed to consider the Security Assessment Plan validated.*

5. REGRESSION TEST

The Quality Control task is also concerned with the control of availability and execution of regression tests for the supported EMI components. Regression tests are useful to retest a previously tested program following modification to ensure that faults have not been introduced as a result of the changes made especially for fixing bugs. As outlined in the *Configuration and Integration guidelines* [R9], regression tests are tests that are meant to verify specific bug fixes and come with any bug reported in the bug tracker. When a new regression test is implemented, it must be documented in the ***Certification report Template*** [R13]. Regression tests should be performed always on a release candidate; exceptions can be done for the release of urgent bug fixes and special occasions agreed within the EMT.

5.1.1 General comments

Although no regression tests have been performed yet, it might be asserted that the instructions on how to implement, execute and document new regression tests are well documented and the procedure looks consolidate. The procedure for handling regression tests is documented in the *Configuration and Integration guidelines* [R9]. At the moment no causes that may lead to unacceptable results are envisaged, but it is strongly encouraged to better clarify how the information on the execution of regression tests should be made available and using which format. The availability of a centralized repository where to maintain relevant information, would really facilitate the QC's work and reduce the possibility of errors. Also consider to extend the *Software Verification and Validation Template* [R13] adding a specific section where details on regression tests can be reported.

6. CONCLUSIONS

This document reports the organization of the QC activity in SA1 and the results of the quality reviews expected for the PM6. The evaluation of SA1 performance, partially based on incomplete measurements, reports that some project's materials (i.e. plans, documents) are not conforming with the quality standards defined in SQAP and many of them are late in their release process. These quality non-conformities will be submitted to QA for further investigation to ensure that no software defects will arise in the future.

Finally, what resulted evident in reviewing the SA1 activity, and in the applicability of QA procedures, is the lack of a centralized place where relevant information is kept and made available to project's stakeholders in a more structured and standardized format. An improvement in the communication system is expected before the next control.