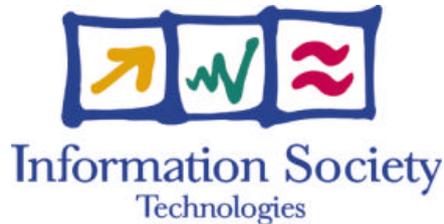


INFORMATION SOCIETY TECHNOLOGIES
(IST)
PROGRAMME



OpenMoIGRID

RISK MANAGEMENT PROCEDURE

Contract Reference:	IST-2001-37238
Document identifier:	OpenMoIGRID-7-D7.1b-0106-1-1-RiskManagementProcedure
Date:	06/09/2003
Work package:	WP 7: Project Management
Partner	UT/OMC
Lead Partner	UT
Document status:	APPROVED
Classification:	INTERNAL
Deliverable identifier:	D7.1b

Abstract: The risk management procedure for the OpenMoIGRID project is a deliverable part of the OpenMoIGRID Quality Plan. The risk management procedure defines rules to identify, estimate, treat and monitor risks.

Delivery Slip

	Name	Partner	Date
From	G DIERCKSEN	OMC	06/09/2003
Verified by	WPMs	all	12/09/2003
Approved by	G.H.F.Diercksen (TC)	OMC	20/09/2003
	R.Ferenczi (QE)	CGX	07/03/2004

Document Log

Issue	Date	Comment	Author
0-0	21/07/2003	Submitted to WPM's	G DIERCKSEN (OMC)
1-1	06/09/2003	Submitted to WPM's	G DIERCKSEN (OMC)

Document Change Record

Issue	Item	Reason for Change
0-0	New document	Reviewers recommendation
1-1		

Files

Files in this section relate to actual storage locations on the project document repository server located at <https://hermes.chem.ut.ee/bscw/bscw.cgi>. The URL below describes the location on project document repository from the root OpenMolGRID directory

Software Products	User files / URL
Word 2000/XP	OpenMolGRID/Workpackage 7/Deliverables/ OpenMolGRID-7-D7.1b-0106-1-1- RiskManagementProcedure

Project information

Project acronym:	OpenMolGRID
Project full title:	Open Computing GRID for Molecular Science and Engineering
Proposal/Contract no.:	IST-2001-37238
European Commission:	
Project Officer:	Annalisa BOGLIOLO
Address:	European Commission - DG Information Society F2 - Grids for Complex Problem Solving B-1049 Brussels Belgium
Office	BU31 4/79
Phone:	+32 2 295 8131
Fax:	+32 2 299 1749
E-mail	annalisa.bogliolo@cec.eu.int
Project Coordinator:	Mathilde ROMBERG
Address:	Forschungszentrum Jülich GmbH ZAM D-52425 Jülich Germany
Phone:	+49 2461 61 3703
Fax:	+49 2461 61 6656
E-mail	m.romberg@fz-juelich.de

CONTENT

1. INTRODUCTION.....	5
1.1. OBJECTIVES OF THIS DOCUMENT	5
1.2. APPLICATION AREA	5
1.3. APPLICABLE DOCUMENTS AND REFERENCE DOCUMENTS.....	5
1.4. DOCUMENT AMENDMENT PROCEDURE.....	5
1.5. TERMINOLOGY.....	5
2. RISK MANAGEMENT ACTIVITIES.....	6
2.1. INTRODUCTION	6
2.2. RISK IDENTIFICATION.....	6
<i>Potential risks</i>	6
<i>Identified risks</i>	6
2.3. RISK ESTIMATION.....	7
<i>Likelihood</i>	7
<i>Severity</i>	7
<i>Level</i>	8
2.4. RISK MITIGATION ACTIVITIES	9
2.5. RISK FOLLOWING-UP: RISK OWNERSHIP, MONITORING AND REPORTING	9
<i>Risk file</i>	9
<i>Indicator of the evolution of risks level</i>	10
3. ANNEX 1: INITIAL POTENTIAL RISKS ANALYSIS.....	11
3.1. INITIAL POTENTIAL RISKS.....	11
<i>Product definition risks</i>	11
<i>Management risks</i>	11
<i>Technical Risks</i>	11

1. Introduction

1.1. Objectives of this document

The aim of this document is to describe the risk management procedure for the OpenMolGRID project.

The risk management procedure for the OpenMolGRID project is a deliverable part of the OpenMolGRID Quality Plan. The risk management procedure defines rules to identify, estimate, treat and monitor risks.

1.2. Application area

The risk management procedure is applicable by all partners. It is applicable throughout the lifetime of the project.

1.3. Applicable documents and reference documents

Applicable documents

[A1] OPENMOLGRID-7-D7.1-0101-1-2 Project Quality Plan

Reference documents

[R1] OpenMolGRID-7-D7.1a-0102-1-1 Project Plan

1.4. Document amendment procedure

Any project partner may request amendments but each amendment must be analysed by the Quality Engineer and then approved by the OpenMolGRID Technical Coordinator and Project Coordinator.

1.5. Terminology

Glossary

EC	European Commission
IST	Information Society Technologies
PC	Project Coordinator
PO	Project Office
SC	Steering Committee
QE	Quality Engineer
PQP	Project Quality Plan
TC	Technical Coordinator
WP	Work Package
WPM	Work Package Manager

2. Risk management activities

2.1. Introduction

The management of risks related to the OpenMolGRID Project consists of the following activities:

1. Risk Identification
2. Risk Estimation
3. Risk Mitigation
4. Risk Follow-up

2.2. Risk Identification

The risk identification process, distinguishes between potential risks and identified risks. A potential risk becomes an identified risk when its characteristics match with criteria defined in §2.3 (Risk estimation).

All OpenMolGRID participants are concerned with risk detection. When a risk is detected, it is reported to the WPM concerned, to the TC and to the QE.

Each time a new risk is detected it shall be managed (identified, assessed, etc) by WP Manager concerned. Nevertheless, the biggest effort has to be put at the beginning in order to anticipate, as far as possible, the monitoring of possible risk and plan, if the case, mitigation actions.

Potential risks

Potential risk identification is made at the beginning of the project and allows the identification of some risks potentially threatening the achievement of project goals. Below in §3, a preliminary analysis of potential risks is presented. The results from this analysis will be updated during the lifetime of the project.

Identified risks

A potential risk becomes an identified risk when its characteristics match with criteria defined in §2.3 (Risk estimation).

In order to help the identification process, project risks will be gathered using the classes listed below.

Risk Class	Characterisation	Management of the Risk
Project Management and organisation	Likelihood of failure to meet development milestones	TC
Product Function	Likelihood of failure to meet product functional requirements	TC
Technical	Likelihood of failure of development process	WPM

Each identified risk refers only to a single class type; nevertheless the same cause may be at the origin of different risks (within the frame of the above classification).

The TC shall create a risk file (Excel spreadsheet, see §0) describing identified risks.

2.3. Risk Estimation

An initial estimation and the relevant justification will be provided under the responsibility of the PC, the TC or WP Manager concerned with the risk.

This risk estimation is carried out on the basis of the likelihood of concerned events and their impact on the project.

Likelihood

Risk likelihood has been classified considering three possible values, namely: low, medium and high.

High (>60%)	If the probability of the risk identified is almost certain.
Medium (between 30 % and 60 %)	The risk is identified. There exists a good opportunity that it will occur.
Low (<30%)	If the probability of the risk is low or if its occurrence is late in relation to the lifetime of the project.

Severity

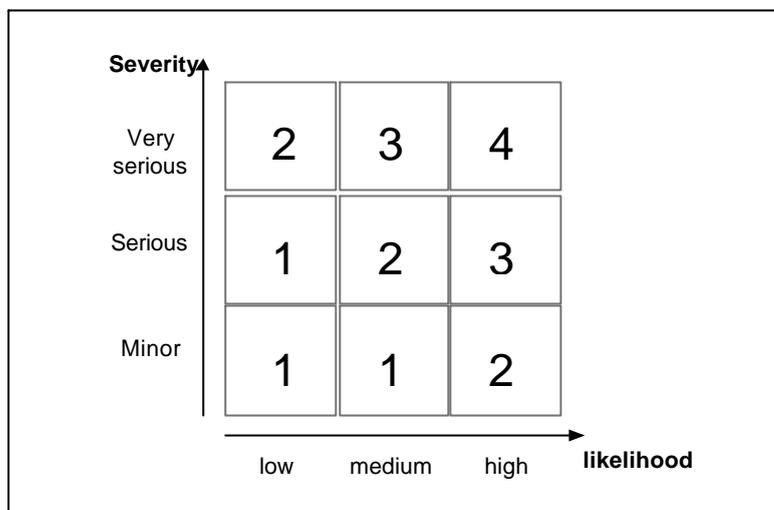
In the same manner the impact evaluation related to each risk has been estimated.

Risks for the project are classified depending on their seriousness according to the following criteria:

Very serious	Uncertainty in the main characteristics of the project (techniques, costs and delays) on the critical path. Failure of a partner.
Serious	Uncertainty on the main contractual requirements (techniques, costs and delays), but without impact on or redefinition of the critical path.
Minor	Impact on the implementation of specific software without affecting the global specification of the project.

Level

Each risk will be referenced within a table having as rows the risk likelihood and as columns the possible impact on the project (see figure below).



Four levels are defined:

Level 1: Low	They are included in the risk file and reviewed by the TC or WP Manager concerned, to check possible variation of its estimations. Actions are evaluated in order to reduce the risk.
Level 2: Medium	An owner is appointed (see: 2.5) to monitor the risk evolution and report to the TC or WP Manager concerned. Actions are evaluated in order to reduce the risk.
Level 3: High	Same as level 2 plus definition of specific mitigation actions. These actions are defined by the TC or WP Manager concerned with the risk, who identifies also possible trigger events to start them. The owner monitors the risks and these trigger events.
Level 4: Critical	Planned mitigation actions are started as scheduled. The risk owner is designated directly by the TC (see: 2.5), who closely monitors the effectiveness of the mitigation actions.

2.4. Risk Mitigation activities

The preventive and corrective treatment consists of suitable actions, to:

- reduce the severity and the probability of occurrence of these risks,
- control the risks.

Unmanageable risks, that is to say risks for which the TC or WPM concerned is not able to deal with in a satisfactory way, shall be highlighted and a proper justification on the lack of mitigation actions should be provided.

Mitigation activity shall be followed-up by the TC or WPM concerned, who supervises the accomplishment and verifies the effectiveness of the performed actions.

These actions are planned for level 3 and level 4 risks and their description will be provided in the risk file.

2.5. Risk Following-up: Risk Ownership, Monitoring and Reporting

Each identified risk shall have an owner who is responsible for its monitoring and reporting.

The TC shall identify the owners for all the risks that have been identified within level 2 and 3.

Level 1 risks do not have an owner. Level 4 risks owners are designated directly by the PC.

In case of ambiguity, the PC will designate risk owner.

Each owner reports periodically to the TC or WPM concerned with (at progress meetings) about the risks under their charge.

The WP Risk files are examined regularly during meetings of advancement of the project.

Risk follow-up is the responsibility of the TC.

Risk file

The TC and each WPM Manager maintains a risk file with a description of their identified risks.

Each risk will contain the following fields:

- Risk identification: WP+sequential number, e.g. WP1-1
- Date of initial detection
- Risk description
- Risk level
- Actions, responsibility, deadline
- Date of last update
- Description of Risk evolution
- Risk date expiry date.

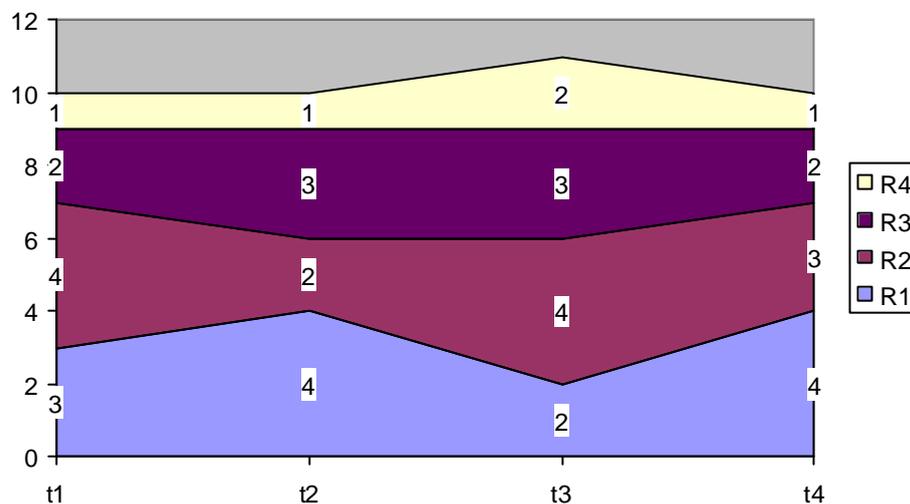
Indicator of the evolution of risks level

The evolution of the level of every risk is represented on a diagram as a function of time.

A graph represents a curve by risk, with:

- in X-axis, the considered dates,
- in Y-axis, the level of every risk that is immediately reported from the curve of risk lower (or of the axis of abscissas, for the first), with the following codification for levels:
 - 1 for the low level,
 - 2 for the middle level,
 - 3 for the high level,
 - 4 for the critical level.

Example:



The lower curve represents the evolution of the level of the risk R1 (coded 3, 4, 2, 4) to dates t1, t2, t3 and t4.

3. ANNEX 1: Initial Potential risks analysis

The analysis of the activities to be carried out in the OpenMolGRID project lists some risks potentially threatening the achievement of project goals. Below a preliminary list of potential risks is presented. The results from this analysis will be monitored and updated during the overall lifetime of the project.

Note: A potential risk becomes an identified risk when its characteristics match with criteria defined in §2.3 (Risk estimation).

3.1. Initial potential risks

Product definition risks

From the product definition point of view, the following initial risks can be listed:

- Mismatch between the OpenMolGRID requirements and the capabilities of UNICORE. The capability of UNICORE to satisfy the requirements coming from the Data Warehouse will impact heavily on the development of the middleware components, modulating the amount of new software to be designed and developed and, eventually, the design of new architectures. This risk is handled by tracing high-level requirements against UNICORE functionality. Close contact with the UNICORE development team is available through FZJ.
- Conflicting requests coming from the two Application areas for the functionalities of the Data Warehouse or for the priorities in its development. This risk is due to the potential conflicts that might arise among requests coming from the two Application areas and to their impact on the Data Warehouse design and development. The TC and the concerned WPM's will identify the areas where such risk is eventually going to arise and follow it up.

Management risks

From the management point of view, the following initial risks can be listed:

- Effectiveness of the overall co-ordination and management structure. The OpenMolGRID project has ambitious technical objectives. The overall co-ordination and the management of interfaces between WPs are hence a critical task and a key to success. To manage this risk, rules and procedures will be established and they will be collected in the PQP.
- Schedule slippage, late deliveries and slow progress in general. This risk is handled by the periodic progress status assessments exchanged between the WPM's and reported to the TC as part of progress reports. Relevant indicators will be defined to cater for trends in progress achievement, showing the average actual schedule slippage of each task with respect to the original planning.
- Under estimation of the required effort. This risk is handled by the WPM's monitoring the planned versus actual effort required by each task. Indicators and statistics will be included in the periodic progress reports to the Project Manager.
- Turn over of key-personnel. This risk is managed by standardising the way of working across the various teams and by defining a backup policy, so that in case of unexpected departure, remaining personnel can temporarily compensate for the absent ones, while waiting for a permanent replacement.
- Late resource availability. The late availability of software, hardware and human resources can be an obstacle to the project's progress. A way of managing this risk is to anticipate requests for resources.

Technical Risks

From the technical point of view, the following initial risks can be listed:

- Unacceptable performance of the final system. The performance of the final system in terms of computers and network facilities could be unacceptable, especially in non-nominal situations.

To manage this risk it is important that early benchmarks are performed simulating the planned applications.