d4science

Project acronym	D4Science
Project full title	**DI**stributed col**L**aboratories **I**nfrastructure on **G**rid **En**abled **T**echnology **4** **Science**
Project No	212488

Deliverable No DNA1.3a

Risk Analysis and Risk Response

August 2008

SEVENTH FRAMEWORK PROGRAMME
Research Infrastructures

INFRA-2007-1.2.2: Deployment of
e-Infrastructures for scientific communities

DOCUMENT INFORMATION

Project	
Project acronym:	D4Science
Project full title:	**DI**stributed col**L**aboratories **I**nfrastructure on **G**rid **EN**abled **T**echnology **4 Science**
Project start:	1st January 2008
Project duration:	24 months
Call:	INFRA-2007-1.2.2: Deployment of e-Infrastructures for scientific communities
Grant agreement no.:	212488
Document	
Deliverable number:	DNA1.3a
Deliverable title:	Risk Analysis and Risk Response
Contractual Date of Delivery:	August 2008
Actual Date of Delivery:	19 November 2008
Editor(s):	L. Candela, P. Pagano
Author(s):	P. Andrade, L. Candela, R. Faggian Marque, J. Michel, P. Pagano
Contributor(s):	Y. Jaques
Reviewer(s):	G. Kakaletris
Participant(s):	ERCIM, CNR, CERN
Work package no.:	NA1
Work package title:	Project Management
Work package leader:	ERCIM
Work package participants:	ERCIM, CNR, CERN
Est. Person-months:	2
Distribution:	Public
Nature:	Report
Version/Revision:	1.0
Draft/Final	Final
Total number of pages: (including cover)	52
Keywords:	Risk Identification, Risk Evaluation, Risk Classification, Risk Plan, Risk Resolution, Risk Monitoring

DISCLAIMER

This document contains description of the D4Science project findings, work and products. Certain parts of it might be under partner Intellectual Property Right (IPR) rules so, prior to using its content please contact the consortium head for approval. E-mail: info@d4science.research-infrastructures.eu

In case you believe that this document harms in any way IPR held by you as a person or as a representative of an entity, please do notify us immediately.

The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated the creation and publication of this document hold any sort of responsibility that might occur as a result of using its content.

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of D4Science consortium and can in no way be taken to reflect the views of the European Union.

The European Union is established in accordance with the Treaty on European Union (Maastricht). There are currently 27 Member States of the Union. It is based on the European Communities and the member states cooperation in the fields of Common Foreign and Security Policy and Justice and Home Affairs. The five main institutions of the European Union are the European Parliament, the Council of Ministers, the European Commission, the Court of Justice and the Court of Auditors. (http://europa.eu.int/)

D4Science is a project partially funded by the European Union

LIST OF ABBREVIATIONS

D4Science	DIstributed colLaboratories Infrastructure on Grid Enabled Technology 4 Science
EC	European Commission
EGEE	Enabling Grids for E-sciencE
JRA	Joint Research Activities
NA	Networking Activities
QATF	Quality Assurance Task Force
SA	Service Activities
VRE	Virtual Research Environment
FARM	Fisheries and Aquaculture Resources Management community
EM	Environmental Monitoring community
ETICS	eInfrastructure for Testing, Integration and Configuration of Software
IR	Information Retrieval
DIR	Distributed Information Retrieval

TABLE OF CONTENTS

DOCUMENT INFORMATION 2
DISCLAIMER 3
LIST OF ABBREVIATIONS 4
TABLE OF CONTENTS 5
LIST OF TABLES 6
LIST OF FIGURES 7
SUMMARY 8
EXECUTIVE SUMMARY 9
1 INTRODUCTION 10
2 THE D4SCIENCE RISK MANAGEMENT METHODOLOGY 12
2.1 Risk Identification Procedure 12
2.2 Risk Evaluation Procedure 13
2.3 Risk Classification Procedure 14
2.4 Risk Planning Procedure 15
2.5 Risk Resolution Procedure 15
2.6 Risk Monitoring Procedure 15
3 RISK ANALYSIS: D4SCIENCE RISKS 16
3.1 Risks Identification 16
3.1.1 Consortium 17
3.1.2 Governing Body 17
3.1.3 Project Activity 18
3.1.4 External 21
3.2 Risks Evaluation 21
3.2.1 Risk Impact 21
3.2.2 Risk Likelihood 34
3.3 Risk Classification 36
4 RISK CONTROL: D4SCIENCE RISKS RESPONSE 41
4.1 Risk Planning 41
4.2 Risk Resolution 43
4.2.1 Consortium Risks Resolution Procedures 43
4.2.2 Governing Body Risks Resolution Procedures 43
4.2.3 Project Activity Risks Resolution Procedures 44
4.2.4 External Risks Resolution Procedures 47
4.3 Risk Monitoring 48
5 CONCLUSIONS 49
GLOSSARY 50
REFERENCES 52

LIST OF TABLES

Table 1. Risk Probability and Impact Rank 13
Table 2. Risk Impact Values 34
Table 3. Risk Likelihood Values 36
Table 4. Risk Exposure Values 40
Table 5. Risk Management Assignment 42

LIST OF FIGURES

Figure 1. D4Science Assets Dependency Graph 37
Figure 2. D4Science Management Structure 41

SUMMARY

The present report is intended to identify, evaluate and classify the actual and potential risks confronted by the D4Science consortium and activities as the project enters the final quarter of the first project year. An appropriate response mechanism is presented for each analysed risk as a result of the risk control methodology put in place. By acknowledging the presence of certain risks, and implementing the preventive recommendations provided herein, project management is in a better position to lead the consortium toward the achievement of the overall project objectives.

EXECUTIVE SUMMARY

The objective of DNA1.3 Risk Analysis and Risk Response is to *analyse* the actual and potential risks confronted by the D4Science consortium and activities and *control* the risks according to the knowledge gained through the analysis. *Risk Analysis* concerns the (i) identification of the risks confronted by the D4Science consortium, governing bodies, internal project activities and external elements employed by the project; (ii) evaluation of the impact of the risk by measuring the probability of the risk occurring and the impact of its occurrence; and (iii) classification of the analysed risks by prioritization according to potential impact and probability of occurrence. *Risk Control* will lead to (i) planning for the management of the risk by identifying relevant actors, tools and actions; (ii) proposing resolution actions per risk; and (iii) monitoring the risks through a dedicated web-based environment.

The document is organised as follows.

Section 1 "Introduction" explains the goal of the Risk Management Activity, and introduces some of the most important risks confronted by the D4Science project.

Section 2 "The D4Science Risk Management Methodology" describes the two main phases of the Risk Management Activity: Risk Analysis and Risk Control. The Risk Analysis methodology is explained in three main steps and these methods are detailed. The Risk Control methodology is explained in three main steps, and these methods are also detailed. It is explained that Risk Analysis activity is to be constantly updated, and Risk Control activity should be monitored by the project's Activity Managers.

Section 3 "Risk Analysis: D4Science Risks" presents the document's findings on Risk Identification, Risk Evaluation and Risk Classification. The actual and potential risks confronted by the D4Science consortium are grouped by "source" of the risk, i.e., consortium, governing body, project activities and external. A total of 25 risks are analysed.

Section 4 "Risk Control: D4Science Risks Response" provides means by which risks, analysed in the previous section, receive an appropriate response through Risk Planning, Risk Resolution and Risk Monitoring. The risks are taken into consideration by first identifying the relevant actors, tools and actions. Specific corrective actions are then proposed per risk, and the concept and operational procedures of an overall web-based monitoring environment is introduced.

Section 5 "Conclusions" completes the deliverable by presenting the main outcomes resulting from the documented activity.

1 INTRODUCTION

Risk can be defined as the combination of the probability of an event and its consequences [4]. Any initiative, activity, organisation or undertaking is exposed to risks since in it there is the potential for events and consequences. Consequences can constitute opportunities for benefits or threats to success but it is common to focus on consequences having negative effects in order for properly react to them. The Risk Management is a structured and organised approach toward risks treatment.

The goal of this deliverable is to design the D4Science Risk Management approach. A Risk Management methodology based on Risk Analysis and Risk Control activities has been adopted. The overall procedure is described in detail in Section 2 that thus forms the core of this document. The results of applying the risk analysis phase to the D4Science scenario are documented in Section 3 while the results of applying the risk control phase are described in Section 4.

D4Science is a large-scale multinational e-Infrastructure project with activities in areas as diverse as training and dissemination, deploying a production infrastructure, and addressing the technical requirements raised by the Environmental Monitoring (EM) and Fisheries and Aquaculture Resources Management (FARM) communities. In the risk identification process, the core activity is the definition of the risk *object,* i.e. a thing to which the specific risk is directed. By carefully considering the project objectives in relation to its *assets*, risk objects are identified. The following D4Science project assets may be considered as targets for risks, and will be detailed in Section 3.1:

- Project-wise achievement;
- Production Infrastructure;
- Virtual Research Environment (VRE);
- Community Tools;
- Community Functionality;
- Community Data;
- gCube Software.

Risks are also associated with a *source,* i.e. the *thing* or event from which the risk comes. Diverse risks to the D4Science project have been identified in the present document and are grouped according to source:

- Consortium:
  - o Consortium undererformance;
  - o Consortium personnel changes;
  - o Dissemination effectiveness underperformance;
- Governing Body:
  - o Management scarce buy-in;
  - o Key user scarce buy-in;
- Project Activity:
  - o Community data rights restrictiveness;
  - o Community low uptake;
  - o Community resources scarce availability;
  - o Requirements poor focus and stability;
  - o gCube implementation delays;
  - o gCube implementation deviation;
  - o Community data deployment deviation;
  - o Community tool deployment deviation;

- Community functionality deployment deviation;
- gCube release availability deviation;
- gCube release poor quality;
- gLite node low availability;
- gCube node low availability;
- Community node low availability;
- VREs functionality poor effectiveness;
- VREs operation deviation;
- VREs availability deviation;

- External:
  - gCube broken dependency;
  - gCube compatibility issue;
  - ETICS availability isse.

Each one of the above identified risks have been evaluated in Section 3.2 by identifying the risk's probability of occurrence and the expected impacted, and finishing by classifying the risks according to a calculated risk exposure ranking. This exercise shows that the most important risks confronting the D4Science project are as follows:

1. VRE Management Implementation Delay;
2. gCube Release Availability Deviation;
3. gCube Implementation Delays;
4. VREs Availability Deviation;
5. Key User Scarce Buy-In; Medium Priority Community Data Deployment Deviation; Community Node Low Availability.

The above risks, as well as all other risks identified and analysed, should be properly managed by implementing the personalised risk resolution procedure recommended in Section 4. A final overall Risk Monitoring procedure, in the form of various web-based tools, is presented in order to observe the status of the risks and to report on them.

2 THE D4SCIENCE RISK MANAGEMENT METHODOLOGY

Risks refer to the potential that a given threat will exploit vulnerabilities of an *asset* or *group of assets* and thereby cause harm to the overall organisation/initiative (in this case the D4Science project). Since risks are factors that prevent the fulfilment of the organisation mission, countermeasures should be prepared to react to adverse events like risks are. A Risk Management Methodology is a set of methods and procedure used to identify both the adverse situations the organisation/initiative is subject to as well as the actions to take in order to identify their happening and consequently react thus to minimise their effect.

The D4Science Risk Management Methodology consists of two main phases: the *Risk Analysis* and *Risk Control* which lead to the definition of the relative methodologies.

The Risk Analysis methodology foresees three main steps:

- **Risk Identification**: it identifies the risks that the different parts of the project (i.e. its assets like the developed or deployed system) are exposed to.
- **Risk Evaluation**: it attaches qualitative and quantitative attributes to the risk, leading to subsequent quantification of the impact (the "damage") that the risk will have in the "value" of the assets.
- **Risk Classification**: it is the core part of the methodology; it identifies the most important risks and promotes in subsequent steps the actions to be taken to safeguard the assets. The prioritization of risks attempts to handle first the risks with greatest impact on the project outcomes and greatest probability of occurrence, and last the risks with lowest impact on the project outcomes and lowest probability of occurrence.

The results of the Risk Analysis activity are included in this report (cf. Section 3). Moreover, it is expected to keep the information contained in this deliverable constantly updated and make available a revised version at the end of project month twenty (August 2009).

The Risk Control methodology also foresees three main steps:

- **Risk Planning:** identifies the actors and the tasks required to control the risks.
- **Risk Resolution:** identifies the strategies to reduce the probability of occurrence of a risk or the countermeasure needed to limit its effects.
- **Risk Monitor:** identifies the procedures and responsibilities to monitor the risks according to the priorities identified in the Risk Classification phase.

It is expected that Risk Control activity is performed by the Activity Managers (cf. Section 4.1). They follow all activities of their area and they are the best candidates to reduce the probability of occurrence of a risk or to implement the required countermeasure. The results of this control activity will be reported in the Quarterly Report document in order to advice the PMB on potential risks.

In the remaining part of this section, the six steps of the Risk Analysis and Risk Control methodologies are described in more detail.

2.1 Risk Identification Procedure

The first part of the Risk Management methodology is about identifying and labelling the risks the project is exposed to. Because of their knowledge of the domain, each task leader of the project is recognised as the best candidate to identify the risks that the assets they are acting on are exposed to.

The labelling of a risk uses the terms *source/problem* and is further explained by the terms *object/impact*, yet not all of them are necessary for the description of a risk. In particular:

- The *source/problem* can be anything external or internal to the project that behaves outside the margins it is expected to behave. Typically these margins should be settled by the specifications; however these are not those that are of interest to our Risk Management, but rather the margins on which the Plan of the project has been settled on. Multiple sources logically combined can form one risk;
- The *object/impact* is always internal to the project. Object can be any element that is affected by a source/problem while the impact is the problem raised in the object, expressed in qualitative and/or quantitative manner.

As an initial indicator, the likelihood of the appearance of the risk can also be attached.

Under the above-mentioned approach, task leaders identify low-level risks and their impact, while subsystem managers identify high-level risks that are not directly conceivable at lower layers.

The challenge however is how to identify the risks in the project. The main sources for obtaining risks are:

- Evaluate the applicability of common risks proposed by various methodologies. Subsequently perform a fine-grained extension of the common risks to the elements of the project that comply with the risk definition;
- Analyse the methodology commonly used by the target communities and evaluate the distance between their approaches and the ones proposed by the project;
- Enumerate all the dependencies of software components and work plans at the task level and enhance this information with the effects caused by the event of failure, delay, misbehaviour (lack of features, performance, etc.).

After the identification of the risks, a number of additional steps have to be performed:

- Identification and removal of duplicated risks;
- Homogenisation of the terminology;
- Sorting of risks according to the source/problem. Multiple effect source/problem can be grouped in one element with multiple objects/impacts.

2.2 Risk Evaluation Procedure

Based on the findings of Risk Identification, all risks identified have to be evaluated. The evaluation of a risk is performed by identifying the Probability of occurrence and the Impact.

The Probability for a particular source/problem to be met is not a strictly mathematical probability factor. For the majority of the risks there are no formulas or there is not enough experimental data to calculate the Probability of occurrence. Thus it is not easily quantifiable.

The Impact measures the damage that will be caused to the object element in case of occurrence of the risk. Again this is not easily quantifiable.

This case of difficult evaluation of the basic metrics of Risk Evaluation is actually typical in IT project where probabilities are estimated by indirect methods such as "expert" opinions, offers, negotiations etc. In the D4Science case, this activity relies on "expert" opinions that evaluate the risks.

Moreover, the terms "Probability Rank" and "Impact Rank" which are more appropriate in the D4Science case are adopted. Probability Rank liberates the analysis from the strict mathematical terms, which in any case is not objectively useful in this context; Impact Rank adds a degree of freedom and uses indirect reference to absolute costs of risk appearance.

Table 1. Risk Probability and Impact Rank

Probability Rank		Impact Rank	
Description	**Value**	**Description**	**Value**
Very Low	1	Doesn't affect the	1

		activity	
Low	2	Affects the activity but a workaround is not needed	2
Medium	3	Affects the activity and it is recommended to put in place a workaround	3
High	4	Affects the activity and it is mandatory to put in place a workaround	4
Very High	5	Affects the activity that has to be consistently rethought	5
Certain	10	Blocks the activity	10

2.3 Risk Classification Procedure

Risk Classification is the main task of the risk analysis. Having the value of the asset that the risk is exposed on, the indicator of likelihood of the risk being triggered, and the impact this will have on the particular asset, it is possible to estimate the importance of the risk. This measurement is typically called Risk Exposure. Since, the Risk Exposure is mathematically calculated as the product of Probability by Impact, it will not be used. Instead the "Risk Exposure Ranking" will be measured to classify risks:

Risk Exposure Ranking = Value of Asset X Probability Ranking X Impact Ranking

To simplify the analysis:

- All elements that do not depend on other assets, hereafter identified as lower level elements, of equal value (e.g. Value of Asset = 1).
- All elements that depend on lower level elements of value C-Value where C-Value is equal to the product of the value of the lower level element by a constant K (K less or equal to 1, e.g. value of K = 0.9); and so on by reducing the value of elements that depend on chain of n assets with respect to elements that depend on n-1 assets.

Two approaches are recommended to sort the classified risks:

- Sort the risks by Probability Rank. This allows focusing on the risks most likely to happen and then investigate the chains they are taking place.
- Sort the risks by Risk Exposure Rank. This captures most serious problems that can affect the asset and then investigate the related events.

Top-ranked risks are identified as System Risks and their environment is described in detail, with respect to:

- Triggering of the risk
- Impact in a qualitative description
- Impact in cost / time equivalents

2.4 Risk Planning Procedure

The Risk Plannning is a task that has to be constantly active. A consistent plan has to be adopted and strictly followed by the assigned persons throughout the duration of the project. This plan involves:

- Setting responsibilities for managing the plan itself;
- Performing periodical updates of the plan;
- Monitoring risks;
- Resolving risks.

The Risk Control activity operates on an enriched set of information already gathered as part of Risk Analysis. In particular, for each risk the following information are in the Risk Plan:

- Description of the risk;
- The situation under which it might occur;
- Ways to monitor the appearance and evolution of the risk;
- Ways to handle the risk upon its appearance including the cost of the countermeasure;
- The responsible for monitoring and handling the risk;

This list is created upon identification of the System Risks, as provided by the Risk Classification process.

2.5 Risk Resolution Procedure

With respect to the resolution of risks, a number of methods can be applied:

- Avoid the occurrence of the risk by reducing/removing the probability of its triggering events;
- Avoid the risk by removing its connection with project activities;
- Transfer the danger to another party or asset with the aim of reducing the probability of occurrence or minimise the impact;
- Acceptance of the risk and implementation of its countermeasure;
- Acceptance of the risk with late reaction;
- Exploitation of risk side effects to balance their impact.

It is obvious that the resolution does not always mean the nullification of a risk's appearance. Rather, depending on the ranking performed, risks of severe impact have to be carefully examined and the countermeasures have to be deeply analysed to ensure that they are capable to limit the effects on the project.

2.6 Risk Monitoring Procedure

The most effective way of monitoring risks is the continuous update of the top-ranked risks of the project. This requires the update of all the relevant contributions and evaluations so that the obtained rank is meaningful. The procedure governing such a kind of activity in the context of the D4Science project is in Section 4.3.

Among the top-ranked risks it is important to implement the actions specified in the Risk Plan on the risks that entered the list since the last evaluation. It is also required to update the status on all other risks. For this purpose, for each risk the following information will be maintained:

- Current position in the top-n ranking;
- Previous position in the top-n ranking;
- Risk description;
- Progress towards resolution.

3 RISK ANALYSIS: D4SCIENCE RISKS

The Risk Analysis methodology identifies and analyzes the risks that can affect the achievement of the D4Science project objectives. As previously outlined the D4Science methodology for controlling the risks consists of three procedures: *(i) Risk Identification* – the risks are identified (cf. Section 3.1), *(ii) Risk Evaluation* – risks impact and likelihood are evaluated (cf. Section 3.2) and *(iii) Risk Classification* – risks are classified according to their exposure ranking (cf. Section 0).

3.1 Risks Identification

In order to provide a better identification and simplify future reference, an unique **ID** and a **Name** are associated to each risk. Each risk also contains a **Description** where more detailed information is provided.

In the risk identification process, the core activity is the definition of the risk ***object***. The risk object can be derived from the project assets. Each risk object is associated to one project asset; each project asset can be linked by one or more risk objects. Analyzing the project objectives the following assets have been identified:

- Project-wise Achievement;
- Production Infrastructure;
  - gLite Node;
  - gCube Node;
  - Community Node;
- Virtual Research Environment (VRE);
- Community Tools;
  - Community High Priority Tool;
  - Community Normal Priority Tool;
  - Community Low Priority Tool;
- Community Functionality;
  - Community High Priority Functionality;
  - Community Normal Priority Functionality;
  - Community Low Priority Functionality;
- Community Data;
  - Community High Priority Data;
  - Community Normal Priority Data;
  - Community Low Priority Data;
- gCube Software;
  - gCore Framework;
  - gCube Information System;
  - gCube Broker and Matchmaker;
  - gCube VO Management;
  - gCube VRE Management;
  - gCube Process Management;
  - gCube Storage, Content, Collection and Metadata Management;
  - gCube Annotation Management;
  - gCube Data Transformation;
  - gCube Archive Import;
  - gCube Index Management;
  - gCube Search Framework;
  - gCube DIR;
  - gCube ASL;
  - gCube Portlets;

Risks are also associated to one ***source*** following the project organization as described in the D4Science Description of Work. The following risk sources have been identified:

- Consortium;
- Governing Body (PMB, PEB);
- Project Activity (JRA, SA, NA);
- External;

In order to allow for a better reading of this section, the identified risks have been grouped in according to their source.

3.1.1 Consortium

ID: Risk1

Name: Consortium Underperformance

Source: Consortium – One or more project partners are not performing as expected and not producing their project outputs according to the agreed upon schedule.

Object: Project-wise Achievement

Description: Partners can underperform with respect to the original plan. Various reasons (limited effort invested, difficulties in personnel/skills retention, late hiring, etc.) can lead to sub-standard contributions and produce delays or damages to the entire consortium by compromising the project achievements.

ID: Risk2

Name: Consortium Personnel Changes

Source: Consortium – One or more project personnel leave or are otherwise unavailable for an extended period of time.

Object: Project-wise Achievement

Description: One or more project personnel leave or are otherwise unavailable for an extended period of time. It is difficult to replace them and get the new employee up to speed.

ID: Risk3

Name: Dissemination Effectiveness Underperformance

Source: Consortium – The project does not disseminate the project objectives and achievements successfully.

Object: Project-wise Achievement

Description: The project's objectives and achievements are not clearly transmitted to outside the consortium.

3.1.2 Governing Body

ID: Risk4

Name: Management Scarce Buy-in

Source: PMB – Lack of support from senior management.

Object: Project-wise Achievement

Description: Senior management are unconvinced by the project and do not interest themselves in encouraging the organization to assist.

ID: Risk5

Name: Key User Scarce Buy-in

Source: PEB – Lack of buy-in from key scientific personnel.

Object: Project-wise Achievement

Description: Key technical personnel from project user communities are unconvinced by the project and do not spend much time testing the results or using the product.

3.1.3 Project Activity

ID: Risk6

Name: Community Data Rights Restrictiveness

Source: NA5/External – Data needed for a VRE community cannot be exploited due to access rights problems.

Object: VRE

Description: Data needed cannot be used due to legal/rights problems or concerns about data privacy and data security.

ID: Risk7

Name: Community Low Uptake

Source: NA5 – Target communities unwilling to change working practices.

Object: VRE

Description: One or more user communities do not change working practices and do not use the provided technology.

ID: Risk8

Name: Community Resources Scarce Availability

Source: NA5 – User community partner cannot meet needs for delivery of requirements, source data, and tools.

Object: VRE

Description: One or more user community partners do not provide the resources they agreed to provide. VOs and VREs suffer from missing data, tools, testers, and users.

ID: Risk9

Name: Requirements Poor Focus and Stability

Source: NA5 – Requirements are not clear or kept stable.

Object: gCube Software

Description: To reach a common understanding on the communities' desiderata among user communities and software engineers is a general issue affecting any software development. Any delay is reaching such a common understanding will result in an unsatisfactory gCube release and will affect the whole project outcome.

ID: Risk10

Name: gCube Implementation Delays

Source: JRA – The implementation of the gCube software is delayed.

Object: gCube Software

Description: JRA implementation is delayed compared to the intended delivery timeline. The risk impact is (non-linearly) analogous to the length of the delay, while the risk likelihood is (non-linearly) reverse analogous. Furthermore some delays can be considered as internal broken dependencies if they exceed the duration of 3 months.

This risk can be decomposed in several sub-risks to reflect the different subsystems that compose the gCube system.

ID: Risk11

Name: gCube Implementation Deviation

Source: JRA – The gCube implementation deviates from the NA5 requirements.

Object: gCube Software

Description: JRA implementation deviates from requirements as expressed via the NA5 activity and validated in JRA activities. In particular, the following gCube services can be affected:

- Search Engine, which has to satisfy the requirements of functionality and performance, depending and exposing the capabilities of the entire system, acting outside its initial scope of Digital Library domain.
- Live Reports, which is a quite innovative (under the perspective of the specific technology and scientific context) and demanding feature of the system.
- Core Layer, which is redesigned for improving functionality, stability and reuse opportunities.
- Content Management, which has to face new requirements for non-typical data management applications and face requirements for grid compliance and high-performance content access operations.
- Presentation Layer, which has to support the provision of user interfaces and match user expectancies while maintaining its ability to be modular and open.
- Archive Import, which has to face diverse type of content repositories not conforming to a single specification.

Excessive deviations can be considered as internal broken dependencies and have to be handled appropriately.

This risk can be decomposed in several sub-risks to reflect the different subsystems that compose the gCube system.

ID: Risk12

Name: Community Data Deployment Deviation

Source: JRA/SA – Data needed for a VRE community cannot be exploited for technical reasons**.**

Object: Community Data

Description: Data needed cannot be imported, stored, or efficiently queried due to technical limitations of either D4Science technology or the source system. The data to deploy can be classified of High, Normal, or Low priority.

ID: Risk13

Name: Community Tools Deployment Deviation

Source: JRA/SA – Tools needed for a VRE community cannot be deployed in the VRE for technical reasons**.**

Object: Community Tools

Description: Tools needed for processing, querying, analysing, and reporting data cannot be deployed on the platform due to technical limitations or incompatibilities of either D4Science technology or the source application. The tools to deploy can be classified of High, Normal, or Low priority.

ID: Risk14

Name: Community Functionality Deployment Deviation

Source: JRA/SA – Functionalities identified by a VRE community cannot be deployed or can only partially be deployed in the VRE for technical or resource reasons**.**

Object: Community Functionality

Description: Functionalities identified by a community as necessary for one VRE cannot be deployed or can only partially be deployed within the D4Science project due to technical or resource (time/money/experience) limitations. The functionality to deploy can be classified of High, Normal, or Low priority.

ID: Risk15

Name: gCube Release Availability Deviation

Source: SA3 - gCube software not released on time.

Object: Production Infrastructure

Description: SA3 does not release the software on time and required updates are not made available to users in the production infrastructure.

ID: Risk16

Name: gCube Release Poor Quality

Source: SA3 - Low quality of gCube releases.

Object: Production Infrastructure

Description: The gCube services made available to the production infrastructure are not reliable due to insufficient or inappropriate testing.

ID: Risk17

Name: gLite Node Low Availability

Source: SA1 - gLite nodes not available or supported.

Object: gLite Node

Description: One or more sites of the production infrastructure do not provide the planned gLite nodes or do not effectively maintain them.

ID: Risk18

Name: gCube Node Low Availability

Source: SA1/SA2 - gCube nodes not available or supported.

Object: gCube Node

Description: One or more sites of the production infrastructure do not provide the planned gCube nodes or do not effectively maintain them.

ID: Risk19

Name: Community Node Low Availability

Source: SA1/SA2 - Community nodes not available or supported.

Object: Community Node

Description: Community nodes registered in the infrastructure and maintained by a user community become unavailable or are not properly maintained.

ID: Risk20

Name: VREs Functionality Poor Effectiveness

Source: SA2/NA5 – Functionalities identified by a VRE community and implemented by the project do not satisfy the expectations.

Object: VRE

Description: Functionalities identified by a community as necessary for one VRE are not satisfied by the delivered implementation.

ID: Risk21

Name: VREs Operation Deviation

Source: SA2/JRA - The creation and management of VREs in the production infrastructure is too complex from the operations perspective.

Object: VRE

Description: The released gCube software cannot be managed by the operation team alone to create VREs. The deployment tools, configuration files, debugging and error logging components do not exist or are not adequate for an effective operation of the infrastructure.

ID: Risk22

Name: VREs Availability Deviation

Source: SA2 - The user communities VREs are not available.

Object: VRE

Description: The user communities Virtual Research Environments are not made available on the expected dates.

3.1.4 External

ID: Risk23

Name: gCube Broken Dependency

Source: External – gCube dependency over external component are broken.

Object: gCube Software

Description: The gCube system depends on a large number of components that might at some point raise dependency problems, either by failing to deliver their functionality or by failing to co-operate with other dependencies. Currently the project heavily depends on: Globus Toolkit WS-Core, EXIST XML DB, Lucene Full Text Index, My SQL Database, Several gLite components (secondary dependencies) and several class libraries.

ID: Risk24

Name: gLite Compatibility Issue

Source: External - The latest development of the gLite middleware prove to be incompatible with the gCube software.

Object: gCube Software

Description: New developments in gLite make their adoption by D4science and exploitation through the gCube software incompatible.

ID: Risk25

Name: ETICS Availability Issue

Source: External - ETICS system not supported or functional.

Object: gCube Software

Description: The ETICS system does not provide the functionality needed or does not support the D4Science build and testing activities.

3.2 Risks Evaluation

The evaluation of risks, as explained in Section 2, consists on the identification of the risk probability of occurrence (likelihood) and the impact.

3.2.1 Risk Impact

Risk	Name	Impact[1]	
Risk1	Consortium Underperformance	4	According to the project Description of Work there are partners responsible of activities and partners that collaborate to implement such activities as result of meetings, discussions, and common

[1] Impact values: 1 – Don't affect the activity; 2 – Affect the activity but a workaround is not needed; 3 – Affect the activity and it is recommended to put in place a workaround; 4 – Affect the activity and it is mandatory to put in place a workaround; 5 – Affect the activity that has to be considerably rethought; 10 – Block the activity.

Risk	Name	Impact[1]	
			agreements. As a consequence, there is a sharing of responsibilities and a distributed load and control in the respect of roles and expertise. Due to the project's size and duration, an under performing partner has an impact potentially on the whole consortium activity and on the project's achievements.
Risk2	Consortium Personnel Changes	3	D4Science is a distributed consortium comprising several partners each having their own rules governing personnel management. Changes in the project staff may affect project scheduling and consequently any project achievement.
Risk3	Dissemination Effectiveness Underperformance	3	The target communities are properly represented in the project and well involved in all project activities. However, the achievements of the project are intended to go beyond the designers and initial consumers to enlarge the potential clients of the D4Science research infrastructure. A dissemination activity performing less well than expected may result in a scarce community awareness of the D4Science findings and scarce opportunity of cross-domain exploitation.
Risk4	Management Scarce Buy-in	4	D4Science is a distributed consortium comprising several partners with their own management. The per partner management directives influence the partner performance. The Can have a strong impact on the sustainability of the project and its general uptake.
Risk5	Key User Scarce Buy-in	4	The D4Science project has been designed to mainly serve the Environmental Monitoring and Fishery and Aquaculture Resources Management. Key representatives of these communities are part of the project itself with the goal to drive the project toward their community needs and validate the resulting system. The concrete exploitation of the D4Science approach depends by this validation. Scarce results in convincing these key representatives

Risk	Name	Impact[1]	
			may have a strong impact on the sustainability of the project and its general uptake.
Risk6	Community Data Rights Restrictiveness	5	The D4Science project will play the role of access point to community data. The data community is interested in are regulated by specific policies. The restrictiveness of these policies may prevent their usage. Depending on the importance of the data the impact may be minimal. Otherwise it may be necessary to seek other data sources or modify the intentions of the affected VREs.
Risk7	Community Low Uptake	5	The D4Science project will serve communities having an in place methodology to achieve their mission by providing them with VREs. Changing the community habits and working environment is a difficult job. The slow adoption of the system by the user communities can result in the provision of limited feedback, the release of less tested software and the lack of usage in the long term.
Risk8	Community Resources Scarce Availability	3	D4Science outcomes effectiveness, mainly the effectiveness of its VREs, strongly depends on the pool of community resources the consortium will have access to. A scarce amount of resources the community is used to may result in an early failure of the project to fulfil the expectations.
Risk9	Requirements Poor Focus and Stability	4	D4Science has been designed to evolve according to community desiderata and promptly react to community requests. The lack of focus and stability in community requests may result in designer's developer's effort and technology waste and scarce user satisfaction.
Risk10	gCube Implementation Delays	10	D4Science outcomes, namely its operational Infrastructure and the existing VREs are based on the gCube technology. Delays in the delivery of this foundational technology and its expected features may result in delays and poorness in the delivered software, the infrastructure and the VREs.

Risk	Name	Impact[1]	
Risk10.1	gCore Implementation Delay	10	gCube, the software supporting the D4Science infrastructure and its VRES, is based on gCore technology. Delays in the delivery of this component and of its expected facilities may have impact on the delivery of the entire gCube system.
Risk10.2	Information System Implementation Delay	10	The gCube Information System is a core component in the gCube Service Oriented system. Delays in the delivery of this component and of its expected facilities may have impact on the delivery of the entire gCube system.
Risk10.3	VRE Management Implementation Delay	10	The gCube VRE Management area is a core component in VRE creation and operation activity. Delays in the delivery of this component and of its expected facilities may have impact on the VRE operation.
Risk10.4	VO Management Implementation Delay	3	The gCube VO Management area is a core component in implementing controlled resource-sharing contexts. Delays in the delivery of this component and of its expected facilities may have impact on the characteristics of the released Infrastructure and VREs. Non-secure Infrastructure and VRE can be deployed and managed without the VO Management set of services.
Risk10.5	Broker and Matchmaker Implementation Delay	3	The gCube Broker and Matchmaker (BM) is a core component in supporting the optimal consumption of available resources at VRE (re-)deployment time. Delays in the delivery of this component and of its expected facilities may have impact on the characteristics of the delivered infrastructure and VREs. VRE can be deployed on a set of gCube nodes a priori identified without the BM.
Risk10.6	Process Management and Optimization Implementation Delay	4	The gCube Process Management area is the component supporting workflow definition and execution in gCube. Delays in the delivery of this component and of its expected facilities may have impact on the delivered VRES. VRE can be deployed without this set of services if the built-in process capabilities are

Risk	Name	Impact[1]	
			deployed with the Search framework.
Risk10.7	Storage, Content, Metadata, and Collection Management Implementation Delay	10	This family of gCube services supports the management of content in gCube. Delays in the delivery of this component and of its expected facilities may have a strong impact on the delivered VREs. VREs cannot function without content space and organisation, while IR facilities are severely impacted without Metadata management.
Risk10.8	Archive Import Implementation Delay	4	The gCube Archive Import area is a core component in supporting the harvesting of existing content. Delays in the delivery of this component and of its expected facilities may have impact on the delivered VREs. Data sources can be imported by interacting directly with the Storage, Content, Metadata, and Collection Management set of services.
Risk10.9	Annotation Management Implementation Delay	2	The gCube Annotation Management area supports the creation of annotations. Delays in the delivery of this component and of its expected facilities may have impact on the delivered VREs from a functional point of view. VRE can be deployed without the annotation capability also.
Risk10.10	Data Transformation Implementation Delay	4	The gCube Data Transformation area supports mechanisms for data changes in form and appearance. Delays in the delivery of this component and of its expected facilities may have impact on the characteristics of the VREs delivered. Data in a specific form can be managed by explicitly providing the system with the proper data.
Risk10.11	DIR Implementation Delay	3	The gCube DIR is a component supporting the search across multiple data sources. Delays in the delivery of this component and of its expected facilities may have limited impact on the delivered VREs. The gCube discovery capability works also without the DIR features but the quality of the results is affected.
Risk10.12	Index Management	10	The gCube Index Management area

Risk	Name	Impact[1]	
	Implementation Delay		supports the creation and management of indices increasing the performance of the retrieval tasks. Delays in the delivery of this component and of its expected facilities may have impact on the characteristics of the delivered VREs. In particular, its absence prohibits the majority of IR functionalities of the VRE.
Risk10.13	Search Framework Implementation Delay	10	The gCube Search Framework is the component orchestrating the content retrieval tasks in gCube. Delays in the delivery of this component and of its expected facilities may have impact on the delivered VREs. All IR facilities are not accessible by the VREs until delivered.
Risk10.14	Application Support Layer Implementation Delay	3	The gCube Application Support Layer is the component abstracting over the gCube service oriented architecture and providing its users with a unique access point. Delays in the delivery of this component and of its expected facilities may have impact on the delivered VREs. VREs user interface delivery is blocked without a workaround.
Risk10.15	Portlets Implementation Delay	5	The gCube Portlets are the constituents of a gCube user interface, each giving access to a set of facilities. Delays in the delivery of any of these components and of its expected facilities may have impact on the delivered VREs. VREs without the user interface implemented by a specific Portlet, and consequently without the relative functions can be deployed.
Risk11	gCube Implementation Deviation	5	gCube evolution is partially based on the community requirements and its validation depends from the amount of requirements satisfied. Deviation from the requirements might compromise the validation of the system from the functional, performance, or security point of view.
Risk11.1	gCore Implementation Deviation	4	gCube, the software supporting the D4Science infrastructure and its VRES, is based on gCore technology. Deviation of this technology from the requirements might compromise the

Risk	Name	Impact[1]	
			gCube system from a functional, performance, or security point of view.
Risk11.2	Information System Implementation Deviation	4	The gCube Information System is a core component in the gCube Service Oriented system. Deviation from requirements might compromise the gCube system from a functional, performance, or security point of view.
Risk11.3	VRE Management Implementation Deviation	4	The gCube VRE Management area is a core component in VRE creation and operation activity. Deviation from the requirements might compromise the effectiveness of this functionality.
Risk11.4	VO Management Implementation Deviation	4	The gCube VO Management area is a core component in implementing controlled resource-sharing contexts. Deviation from the requirements might compromise the effectiveness of this functionality. Non secure VRE can be deployed and managed without the VO Management set of services.
Risk11.5	Broker and Matchmaker Implementation Deviation	2	The gCube Broker and Matchmaker (BM) is a core component in supporting the optimal consumption of available resources at VRE (re-)deployment time. Deviation from the requirements might compromise the effectiveness of this functionality. VRE can be deployed on a set of gCube nodes a priori identified.
Risk11.6	Process Management and Optimization Implementation Deviation	3	The gCube Process Management area is the component supporting workflow definition and execution in gCube. Deviation from the requirements might compromise the effectiveness of this functionality. VRE can be deployed without this set of services if the built-in process capabilities are deployed with the Search framework.
Risk11.7	Storage, Content, Metadata, and Collection Management Implementation Deviation	4	This family of gCube services supports the management of content in gCube. Deviations from the requirements might compromise the effectiveness of this functionality and have a strong impact on the delivered VREs.

Risk	Name	Impact[1]	
Risk11.8	Archive Import Implementation Deviation	3	The gCube Archive Import area is a core component in supporting the harvesting of existing content. Deviation from the requirements might compromise the effectiveness of this functionality and have impact on the delivered VREs. Data sources can be imported by interacting directly with the Storage, Content, Metadata, and Collection Management set of services.
Risk11.9	Annotation Management Implementation Deviation	2	The gCube Annotation Management area supports the creation of annotations. Deviation from the requirements might compromise the effectiveness of this functionality and have impact on the delivered VREs. VRE can be deployed without the annotation capability.
Risk11.10	Data Transformation Implementation Deviation	3	The gCube Data Transformation area supports mechanisms for data changes in form and appearance. Deviation from the requirements might compromise the effectiveness of this functionality and have impact on the delivered VREs. Data in a specific form can be managed by explicitly providing the system with the proper data.
Risk11.11	DIR Implementation Deviation	3	The gCube DIR is a component supporting the search across multiple data sources. Deviation from the requirements might compromise the effectiveness of this functionality. The discovery capability also works without the DIR features but the quality of the results is affected.
Risk11.12	Index Management Implementation Deviation	4	The gCube Index Management area supports the creation and management of indices increasing the performance of the retrieval tasks. Deviation from the requirements might impact on performance, stability or functionality of the IR subsystem, yet the rest of the system can be operational within limits.
Risk11.13	Search Framework Implementation Deviation	4	The gCube Search Framework is the component orchestrating the content retrieval tasks in gCube. Deviation from the requirements might

Risk	Name	Impact[1]	
			compromise the effectiveness of this core VRE functionality.
Risk11.14	Application Support Layer Implementation Deviation	3	The gCube Application Support Layer is the component abstracting over the gCube service oriented architecture and providing its users with a unique access point. Deviation from the requirements might compromise the effectiveness of this core VRE functionality. User interface functionality and performance might be impacted despite direct access to native gCube services can reduce this impact.
Risk11.15	Portlets Implementation Deviation	3	The gCube Portlets are the constituents of a gCube user interface, each giving access to a set of facilities. Deviation from the requirements might compromise the effectiveness of the overall VRE.
Risk12	Community Data Deployment Deviation	4	Through VRE communities are expected to have access to all the data sources they are used to deal with. Deviation from the requirements might prevent the effectiveness of the delivered VREs and, in general, the buy-in of the D4Science technology. The lack of a small percentage of the data sources a VRE is intended to give access to might not result in an invalidation of the whole VRE. Depending on the data source value/significance it may be vital to find a workaround.
Risk12.1	High Priority Community Data Deployment Deviation	5	Through VRE communities are expected to have access to all the data sources they are used to deal with. Among these data sources there are some particularly relevant with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these data sources might have strong impact on the effectiveness of the related VREs.
Risk12.2	Medium Priority Community Data Deployment Deviation	4	Through VRE communities are expected to have access to all the data sources they are used to deal with. Among these data sources there are some of medium importance with respect to the community scenarios (the relevance

Risk	Name	Impact[1]	
			is indicated by the community itself). Deviations from requirements about these data sources might have impact on the effectiveness of the related VREs.
Risk12.3	Low Priority Community Data Deployment Deviation	2	Through VRE communities are expected to have access to all the data sources they are used to deal with. Among these data sources there are some of secondary importance with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these data sources might have limited impact on the effectiveness of the related VREs.
Risk13	Community Tools Deployment Deviation	4	Through VRE communities are expected to have access to all the tools they are used to deal with. Depending on the tools capabilities for data import the impact may be minimal as the user can access VRE data and import it into the tool locally. Some tools may be of lower importance and their non-availability may have a minimal impact. In other cases it may be a significant impediment to the functional requirements of a VRE and it then may be vital to find a workaround.
Risk13.1	High Priority Community Tool Deployment Deviation	5	Through VRE communities are expected to have access to all the tools they are used to deal with. Among these tools there are some particularly relevant with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these tools might have strong impact on the effectiveness of the related VREs.
Risk13.2	Medium Priority Community Tool Deployment Deviation	4	Through VRE communities are expected to have access to all the tools they are used to deal with. Among these tools there are some of medium importance with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these tools might have impact on the effectiveness of the related VREs.

Risk	Name	Impact[1]	
Risk13.3	Low Priority Community Tool Deployment Deviation	2	Through VRE communities are expected to have access to all the tools they are used to deal with. Among these tools there are some of secondary importance with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these tools might have limited impact on the effectiveness of the related VREs.
Risk14	Community Functionality Deployment Deviation	4	Through VRE communities are expected to have access to a set of functionality. Depending on the functionality the impact may be minimal as the user can access VRE data and process it locally. Some functionality is of lower importance and their non-availability may have a minimal impact. In other cases they may block VRE acceptance or community uptake, in which case it is vital to find a workaround.
Risk14.1	High Priority Community Functionality Deployment Deviation	5	Through VRE communities are expected to have access to a set of functionality. Among these there are some particularly relevant with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these functionality might have strong impact on the effectiveness of the related VREs.
Risk14.2	Medium Priority Community Functionality Deployment Deviation	4	Through VRE communities are expected to have access to a set of functionality. Among these there are some of medium importance with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these functionality might have impact on the effectiveness of the related VREs.
Risk14.3	Low Priority Community Functionality Deployment Deviation	2	Through VRE communities are expected to have access to a set of functionality. Among these there are some of secondary importance with respect to the community scenarios (the relevance is indicated by the community itself). Deviations from requirements about these

Risk	Name	Impact[1]	
			functionality might have limited impact on the effectiveness of the related VREs.
Risk15	gCube Release Availability Deviation	10	The gCube technology has to pass a building and testing phase before to be used in the production infrastructure. Deviation or delays in this activity will result in the newly implemented functionality or software to be deployed in late in the infrastructure by SA1, and a potential delay for the NA activities.
Risk16	gCube Release Poor Quality	4	The gCube technology has to pass a building and testing phase aiming to certify its quality before to be used in the production infrastructure. The scarce effectiveness of the testing phase might result in the release of software of poor quality. Some functionality exposed to the users might be unreliable or unsatisfactory. This could have an impact on the work of the users and their trust on the infrastructure and services provided.
Risk17	gLite Node Low Availability	2	D4Science has its own gLite nodes and rely on EGEE to have access to other gLite nodes. The EGEE production infrastructure provides a large set of resources spread through more then 250 sites. The EGEE middleware is designed to dynamically add/remove resources to/from the EGEE grid infrastructure. The unavailability of some gLite nodes provided by the D4Science is therefore not significant when comparing with the number of gLite sites of the EGEE infrastructure.
Risk18	gCube Node Low Availability	4	gCube nodes are the basic constituents of a gCube based infrastructure since they host gCube services. The unavailability of one gCube node can compromise the availability of the infrastructure if the services running on that node are not replicated. In this situation these services must be restored in another node of the infrastructure.
Risk19	Community Node Low Availability	4	Community nodes are those node originally hosting data sources or tools the community is interested in. The unavailability of a community

Risk	Name	Impact[1]	
			node can partially or completely compromise the functionality of the VRE that exploits the services or data deployed on such node.
Risk20	VRE Functionality Poor Effectiveness	4	Community requirements may be related to specific functional enhancement/customisation. The unavailability or lack of effectiveness of a customised service can compromise partially or completely the functionality of the VRE that is designed to exploit that service.
Risk21	VREs Operation Deviation	5	The operation of VREs should be a task simplified by the support of gCube technology. Deviations from this expectation might result in poor quality of service of the delivered VREs. This would require additional effort to improve the operational aspects of the software (gCube) and services provided, as well to adapt the support procedure in order to ensure the availability services promised to the user communities.
Risk22	VREs Availability Deviation	10	Each VRE should be 24/7 operational during its specified lifetime. The (temporary) unavailability of a VRE would delay the exploitation and dissemination work of the related user community.
Risk23	gCube Broken Dependency	4	gCube is a component oriented software that rely on some off-the-shelf other software components. The unavailability of one of these off-the-shelf technologies might prevent some of the gCube components to work properly. This will impact on the gCube functionality.
Risk24	gLite Compatibility Issue	4	gCube relies on gLite technology for what is concerned with the access to a Grid infrastructure based on such a software, namely EGEE. This is a sort of off-the-shelf technology that evolves according to its own development cycle. Newest version of such a technology might result not compatible with the gCube technology. This imposes revision of the gCube technology in order to guarantee the interaction with a gLite based technology.

Risk	Name	Impact[1]	
Risk25	ETICS Availability Issue	5	D4Science (SA3 activity) relies on ETICS technology for what is concerned with the gCube build and integration activity. This is a sort of off-the-shelf technology that evolves according to its own development cycle. Missing functionality or limited support from ETICS might block the SA3 activity and consequently the delivery of gCube enhanced versions aiming to improve the effectiveness of the D4Science infrastructure and the relative VREs.

Table 2. Risk Impact Values

3.2.2 Risk Likelihood

Risk	Risk Name	Likelihood[2]
Risk1	Consortium Underperformance	1
Risk2	Consortium Personnel Changes	3
Risk3	Dissemination Effectiveness Underperformance	2
Risk4	Management Scarce Buy-in	2
Risk5	Key User Scarce Buy-in	3
Risk6	Community Data Rights Restrictiveness	2
Risk7	Community Low Uptake	3
Risk8	Community Resources Scarce Availability	2
Risk9	Requirements Poor Focus and Stability	3
Risk10	gCube Implementation Delays	3
Risk10.1	gCore Implementation Delay	1
Risk10.2	Information System Implementation Delay	1
Risk10.3	VRE Management Implementation Delay	2
Risk10.4	VO Management Implementation Delay	2
Risk10.5	Broker and Matchmaker Implementation Delay	3
Risk10.6	Process Management and Optimization Implementation Delay	3
Risk10.7	Storage, Content, Metadata, and Collection Management Implementation Delay	2
Risk10.8	Archive Import Implementation Delay	4

[2] Likelihood values: 1 – Very Low; 2 – Low; 3 – Medium; 4 – High; 5 – Very High; 10 – Certain.

Risk	Risk Name	Likelihood[2]
Risk10.9	Annotation Management Implementation Delay	2
Risk10.10	Data Transformation Implementation Delay	3
Risk10.11	DIR Implementation Delay	2
Risk10.12	Index Management Implementation Delay	2
Risk10.13	Search Framework Implementation Delay	1
Risk10.14	Application Support Layer Implementation Delay	3
Risk10.15	Portlets Implementation Delay	3
Risk11	gCube Implementation Deviation	2
Risk11.1	gCore Implementation Deviation	1
Risk11.2	Information System Implementation Deviation	2
Risk11.3	VRE Management Implementation Deviation	2
Risk11.4	VO Management Implementation Deviation	2
Risk11.5	Broker and Matchmaker Implementation Deviation	2
Risk11.6	Process Management and Optimization Implementation Deviation	2
Risk11.7	Storage, Content, Metadata, and Collection Management Implementation Deviation	2
Risk11.8	Archive Import Implementation Deviation	3
Risk11.9	Annotation Management Implementation Deviation	2
Risk11.10	Data Transformation Implementation Deviation	3
Risk11.11	DIR Implementation Deviation	2
Risk11.12	Index Management Implementation Deviation	2
Risk11.13	Search Framework Implementation Deviation	2
Risk11.14	Application Support Layer Implementation Deviation	3
Risk11.15	Portlets Implementation Deviation	3
Risk12	Community Data Deployment Deviation	3
Risk12.1	High Priority Community Data Deployment Deviation	2
Risk12.2	Medium Priority Community Data Deployment Deviation	2
Risk12.3	Low Priority Community Data Deployment Deviation	4
Risk13	Community Tools Deployment Deviation	3

Risk	Risk Name	Likelihood[2]
Risk13.1	High Priority Community Tool Deployment Deviation	2
Risk13.2	Medium Priority Community Tool Deployment Deviation	3
Risk13.3	Low Priority Community Tool Deployment Deviation	4
Risk14	Community Functionality Deployment Deviation	3
Risk14.1	High Priority Community Functionality Deployment Deviation	2
Risk14.2	Medium Priority Community Functionality Deployment Deviation	2
Risk14.3	Low Priority Community Functionality Deployment Deviation	3
Risk15	gCube Release Availability Deviation	4
Risk16	gCube Release Poor Quality	3
Risk17	gLite Node Low Availability	2
Risk18	gCube Node Low Availability	2
Risk19	Community Node Low Availability	3
Risk20	VRE Functionality Poor Effectiveness	2
Risk21	VREs Operation Deviation	3
Risk22	VREs Availability Deviation	4
Risk23	gCube Broken Dependency	2
Risk24	gLite Compatibility Issue	1
Risk25	ETICS Availability Issue	1

Table 3. Risk Likelihood Values

3.3 Risk Classification

As introduced in Section 2, risks are classified according to their Risk Exposure Ranking. This value is calculated from the formula below:

Risk Exposure Ranking = Value of Asset X Likelihood X Impact

Section 3.2 defines the Likelihood and Impact associated to each risk. In Section 3.1 each risk is associated to one risk Object. As already explained the risk Object is always one of the project assets. To calculate the value of such asset, the dependencies among assets must be taken in consideration:

- Assets with no dependencies:
  - Asset value = 1
- Assets with dependencies:
  - Asset value = asset value of the dependency * 0.9

The following figure represents the dependencies between the project assets.

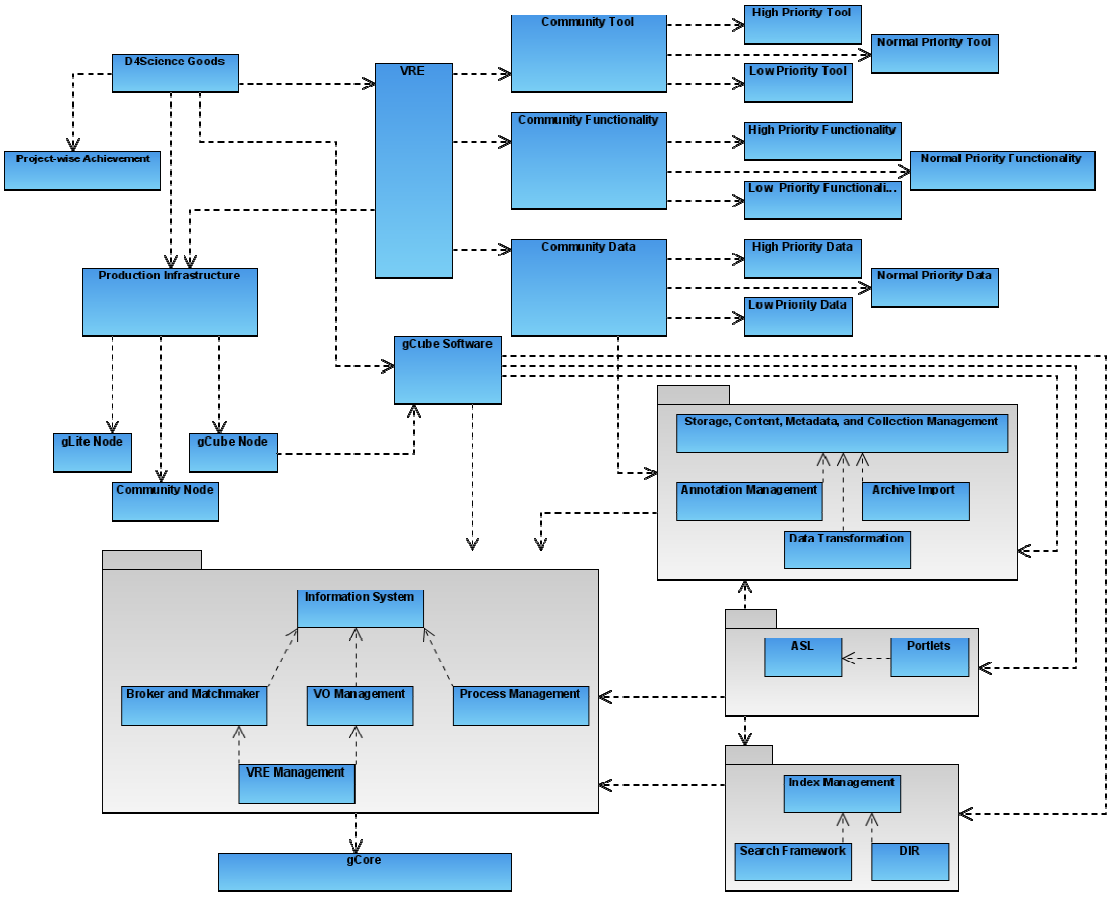

Figure 1. D4Science Assets Dependency Graph

From the dependency graph of Figure 1 it is possible to calculate the asset value for each risk identified in Section 3.1. These values are presented in Table 4 that also presents the impact, the likelihood, and finally the risk exposure ranking associated to each risk.

ID	Name	Value	Impact[3]	Likelihood[4]	Exposure
Risk1	Consortium Underperformance	1.00	4	1	**4.0**
Risk2	Consortium Personnel Changes	1.00	3	3	**9.0**
Risk3	Dissemination Effectiveness Underperformance	1.00	3	2	**6.0**
Risk4	Management Scarce Buy-in	1.00	4	2	**8.0**
Risk5	Key User Scarce Buy-in	1.00	4	3	**12.0**

[3] Impact values: 1 – Doesn't affect the activity; 2 – Affects the activity but a workaround is not needed; 3 – Affects the activity and it is recommended to put in place a workaround; 4 – Affects the activity and it is mandatory to put in place a workaround; 5 – Affects the activity that has to be considerably rethought; 10 – Blocks the activity.
[4] Likelihood values: 1 – Very Low; 2 – Low; 3 – Medium; 4 – High; 5 – Very High; 10 – Certain.

ID	Name	Value	Impact[3]	Likelihood[4]	Exposure
Risk6	Community Data Rights Restrictiveness	0.35	5	2	**3.5**
Risk7	Community Low Uptake	0.35	5	3	**5.2**
Risk8	Community Resources Scarce Availability	0.35	3	2	**2.1**
Risk9	Requirements Poor Focus and Stability	0.48	4	3	**5.7**
Risk10	gCube Implementation Delays	0.48	10	3	**14.3**
Risk10.1	gCore Implementation Delay	1.00	10	1	**10.0**
Risk10.2	Information System Implementation Delay	0.73	10	1	**7.3**
Risk10.3	VRE Management Implementation Delay	0.90	10	2	**18.0**
Risk10.4	VO Management Implementation Delay	0.81	3	2	**4.9**
Risk10.5	Broker and Matchmaker Implementation Delay	0.81	3	3	**7.3**
Risk10.6	Process Management and Optimization Implementation Delay	0.81	4	3	**9.7**
Risk10.7	Storage, Content, Metadata, and Collection Management Implementation Delay	0.59	10	2	**11.8**
Risk10.8	Archive Import Implementation Delay	0.66	4	4	**10.5**
Risk10.9	Annotation Management Implementation Delay	0.66	2	2	**2.6**
Risk10.10	Data Transformation Implementation Delay	0.66	4	3	**7.9**
Risk10.11	DIR Implementation Delay	0.66	3	2	**3.9**
Risk10.12	Index Management Implementation Delay	0.59	10	2	**11.8**
Risk10.13	Search Framework Implementation Delay	0.66	10	1	**6.6**
Risk10.14	Application Support Layer Implementation Delay	0.53	3	3	**4.7**
Risk10.15	Portlets Implementation Delay	0.53	5	3	**8.0**
Risk11	gCube Implementation Deviation	0.48	5	2	**4.8**
Risk11.1	gCore Implementation Deviation	1.00	4	1	**4.0**
Risk11.2	Information System Implementation Deviation	0.73	4	2	**5.8**

ID	Name	Value	Impact[3]	Likelihood[4]	Exposure
Risk11.3	VRE Management Implementation Deviation	0.90	4	2	**7.2**
Risk11.4	VO Management Implementation Deviation	0.81	4	2	**6.5**
Risk11.5	Broker and Matchmaker Implementation Deviation	0.81	2	2	**3.2**
Risk11.6	Process Management and Optimization Implementation Deviation	0.81	3	2	**4.9**
Risk11.7	Storage, Content, Metadata, and Collection Management Implementation Deviation	0.59	4	2	**4.7**
Risk11.8	Archive Import Implementation Deviation	0.66	3	3	**5.9**
Risk11.9	Annotation Management Implementation Deviation	0.66	2	2	**2.6**
Risk11.10	Data Transformation Implementation Deviation	0.66	3	3	**5.9**
Risk11.11	DIR Implementation Deviation	0.66	3	2	**3.9**
Risk11.12	Index Management Implementation Deviation	0.59	4	2	**4.7**
Risk11.13	Search Framework Implementation Deviation	0.66	4	2	**5.2**
Risk11.14	Application Support Layer Implementation Deviation	0.53	3	3	**4.8**
Risk11.15	Portlets Implementation Deviation	0.53	3	3	**4.8**
Risk12	Community Data Deployment Deviation	0.53	4	3	**6.4**
Risk12.1	High Priority Community Data Deployment Deviation	1.00	5	2	**10.0**
Risk12.2	Medium Priority Community Data Deployment Deviation	1.00	4	2	**8.0**
Risk12.3	Low Priority Community Data Deployment Deviation	1.00	2	4	**8.0**
Risk13	Community Tools Deployment Deviation	0.90	4	3	**10.8**
Risk13.1	High Priority Community Tool Deployment Deviation	1.00	5	2	**10.0**
Risk13.2	Medium Priority Community Tool Deployment Deviation	1.00	4	3	**12.0**
Risk13.3	Low Priority Community Tool Deployment Deviation	1.00	2	4	**8.0**
Risk14	Community Functionality	0.90	4	3	**10.8**

ID	Name	Value	Impact[3]	Likelihood[4]	Exposure
	Deployment Deviation				
Risk14.1	High Priority Community Functionality Deployment Deviation	1.00	5	2	**10.0**
Risk14.2	Medium Priority Community Functionality Deployment Deviation	1.00	4	2	**8.0**
Risk14.3	Low Priority Community Functionality Deployment Deviation	1.00	2	3	**6.0**
Risk15	gCube Release Availability Deviation	0.39	10	4	**15.5**
Risk16	gCube Release Poor Quality	0.39	4	3	**4.6**
Risk17	gLite Node Low Availability	1.00	2	2	**4.0**
Risk18	gCube Node Low Availability	0.43	4	2	**3.4**
Risk19	Community Node Low Availability	1.00	4	3	**12.0**
Risk20	VRE Functionality Poor Effectiveness	0.35	4	2	**2.8**
Risk21	VREs Operation Deviation	0.35	5	3	**5.2**
Risk22	VREs Availability Deviation	0.35	10	4	**13.9**
Risk23	gCube Broken Dependency	0.48	4	2	**3.8**
Risk24	gLite Compatibility Issue	0.48	4	1	**1.9**
Risk25	ETICS Availability Issue	0.48	5	1	**2.4**

Table 4. Risk Exposure Values

4 RISK CONTROL: D4SCIENCE RISKS RESPONSE

The Risk Control methodology provides means by which identified risks are systematically evaluated and, whenever a risk occur, to put in place the corrective actions and plans to control the identified risk and minimise its impact on the project assets. As previously outlined the D4Science methodology for controlling the risks consists of three procedures: *Risk Planning* (cf. Section 4.1), *Risk Resolution* (cf. Section 4.2) and *Risk Monitoring* (cf. Section 4.3).

4.1 Risk Planning

The procedure governing the Risk Planning is, once the have been identified and properly classified, the procedure regulating the rest of the risk management activity and thus it must be active for the whole duration of the project. Such a procedure mainly consists in identifying *(i)* the *actors*, i.e. who will do what, *(ii)* the *tools*, i.e. which instruments actors will use, and *(iii)* the *actions*, i.e. what sequence of actions will be taken to monitor the risk and minimise its impact.

For what concerns the ***actors***, Figure 2 shows the overall project management structure. Since the risk management is a typical managerial activity, it is expected that the appointed managers take care of such an activity. Moreover, since different managers will be responsible for different activities, it is expected that each of them will take care of the risk related to such activities.

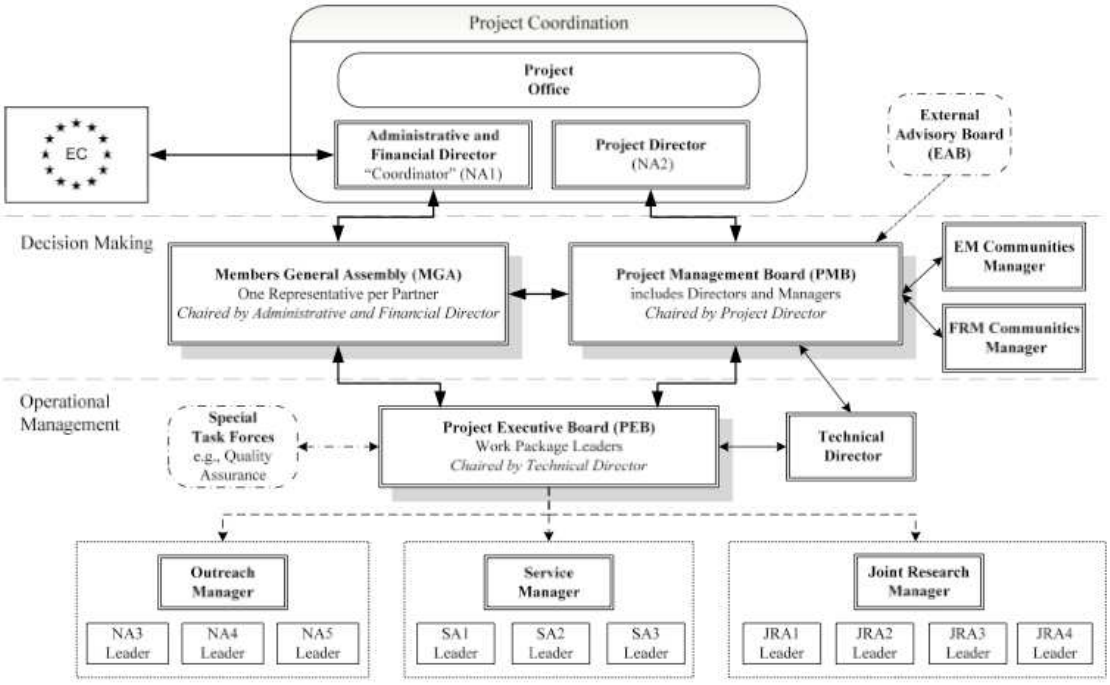

Figure 2. D4Science Management Structure

In D4Science, the overall project coordination is split between an *Administrative and Financial Director* (Jessica Michel) and a *Project Director* (Donatella Castelli). These Directors will jointly take care of the risks related to the consortium (Risk1-5). Moreover, because of their role they will be informed on the status of all the rest of risks.

The concrete activities of the project fall each in one of the three classes the project is organised in. The coordination of each of these classes is assigned to a Manager: an *Outreach Manager* (Johannes Keizer), a *Service Manager* (Roberta Faggian Marque) and a *Joint Research Manager* (George Kakaletris). Moreover, the set of managers is

completed by *(i)* an *EM*[5] *Community Manager* (Luigi Fusco) and a *FARM*[6] *Community Manager* (*Marc Taconet*), i.e. the managers appointed to organise the activities from the relative communities perspective, and *(ii)* a *Technical Director* (Pasquale Pagano) that supervises all the activities to guarantee the overall coordination of what concerns the technical aspects. Each Manager is the primary responsible for managing the risks related to its activities.

Risk Management responsibilities are summarised in Table 5.

Table 5. Risk Management Assignment

Actor	Managed Risk
Administrative and Financial Director	*Primary:* Risk1, Risk2, Risk3, Risk4, Risk5 *Secondary*: All
Project Director	*Primary:* Risk1, Risk2, Risk3, Risk4, Risk5 *Secondary*: All
Technical Director	*Secondary*: All
Outreach Manager	*Primary:* Risk3, Risk6, Risk7, Risk8, Risk9 *Secondary*: All
Service Manager	*Primary:* Risk15, Risk16, Risk17, Risk18, Risk19, Risk20, Risk21, Risk22, Risk25 *Secondary*: Risk7, Risk10
Joint Research Manager	*Primary:* Risk10, Risk11, Risk23, Risk24 *Secondary*: Risk6, Risk9
EM Community Manager	*Primary:* Risk12, Risk13, Risk14 *Secondary*: Risk15, Risk17, Risk18, Risk19, Risk20, Risk21, Risk22
FARM Community Manager	*Primary:* Risk12, Risk13, Risk14 *Secondary*: Risk15, Risk17, Risk18, Risk19, Risk20, Risk21, Risk22

For what concerns the **tools**, it was decided to rely on the tools already deployed to serve the project, namely the *(i)* the Wiki supporting the project Quality-related activities[7] – for publishing information about the risks, *(ii)* the Collaborative Working Space[8] – to support the cooperation between the involved actors by promoting the exchange of documents and the like related to the risk management activities, and *(iii)* the NA1 mailing list. The usage of these tools is reported in the procedures they are supporting, namely the Risk Monitoring (cf. Section 4.3)

For what concerns the **actions**, they are related to the Risk Monitoring and Risk Resolution procedures. In particular, each of the actors involved in the Risk Management procedure as described above is requested *(i)* to implement the Risk Monitoring procedure for the Risks for which they are the *primary responsible* and *(ii)* to notify the Project Management Board (PMB) whenever a Risk they are responsible for monitoring occurs by providing this board with information documenting the risk occurrence and the relative countermeasures identified in the Risk Resolution part of this report (cf. Section 4.2).

[5] EM stands for Environmental Monitoring.
[6] FARM stands for Fishery and Aquaculture Resources Management.
[7] https://quality.wiki.d4science.research-infrastructures.eu/
[8] http://bscw.d4science.research-infrastructures.eu/

4.2 Risk Resolution

This section reports corrective actions to be performed whenever the relative risk occurs. Such resolution actions are specific for each risk and thus a per-risk description is provided. It is important to notice that these corrective actions have a cost and that the diverse corrective actions/procedures with different costs can be put in place to attack the same risk. The one reported below has been identified by carefully evaluating various aspects including the impact of the risk, the cost of the actions and the characteristics of the context, i.e. the D4Science project. Moreover, these procedures can partially resolve/mitigate the risk or generate another risk. Risks are organised by source: Consortium-related Risks (cf. Section 4.2.1), Governing Body-related Risks (cf. Section 4.2.2), Project Activity-related Risks (cf. Section 4.2.3), External Risks (cf. Section 4.2.4).

4.2.1 Consortium Risks Resolution Procedures

ID: Risk1

Name: Consortium Underperformance

Resolution: Careful monitoring of the progresses produced by each partner has to be put in place. Common metrics have to be used to measure periodically the partners' productivity and efficacy. The escalation procedures identified by the Quality Assurance Task Force have to be put in place at the first evidence of potential problems introduced by inaccuracy or delays of a partner. For what is concerned with the cost of these actions, it corresponds to the effort needed to manage a consortium consisting of various partner spread over various Institutions.

ID: Risk2

Name: Consortium Personnel Changes

Resolution: Determine plans of key personnel and adjust accordingly. Strong project documentation to minimize loss of project knowledge. For what is concerned with the cost of these actions, it corresponds to the effort needed to manage a potentially dynamic team with a recognised know-how.

ID: Risk3

Name: Dissemination Effectiveness Underperformance

Resolution: Organisation of and participation to focussed meetings and large conferences have to be encouraged in the consortium and supported to disseminate as large as possible the different results achieved by the project. The dissemination material will be revised internally to the consortium to improve its effectiveness. In particular, this material will be revised before its exploitation as well as after the exploitation thus to take into account the feedback received. New dissemination material will be produced whenever the existing one is not considered well enough to meet the user expectations. For what is concerned with the cost of these actions, it corresponds to the effort needed to disseminate project outcomes in a qualitative manner.

4.2.2 Governing Body Risks Resolution Procedures

ID: Risk4

Name: Management Scarce Buy-in

Resolution: Determine key managers and attempt to get early buy-in. Recruit new and skilled managers, i.e. people having proven and true expertise with respect to the role they will cover. For what is concerned with the cost of these actions, it can vary from the effort needed to initially raise interests and expectations in key partners to the one recruiting one.

ID: Risk5

Name: Key User Scarce Buy-in

Resolution: Determine key players in target communities and attempt to get early buy-in. Recruit community key representatives, i.e. people having strong impact on the community behaviour and operation. For what is concerned with the cost of these actions, it can vary from the effort needed to initially raise interests and expectations in key partners to the one recruiting one.

4.2.3 Project Activity Risks Resolution Procedures

ID: Risk6

Name: Community Data Rights Restrictiveness

Resolution: Convince data holder of the steps taken for data security; agree to maintain data products strictly private; see if more aggregate products are less sensitive; find alternative data source from different provider. For what is concerned with the cost of these actions, it can vary a lot depending from the effectiveness of the project partners to raise interest around the D4Science infrastructure and its effectiveness in guaranteeing proper data usage.

ID: Risk7

Name: Community Low Uptake

Resolution: Determine key players in target communities and attempt to get early buy-in. Recruit community key representatives, i.e. people having strong impact on the community behaviour and operation. Improve dissemination and training. For what is concerned with the cost of these actions, it can vary from the effort needed to initially raise interests and expectations in key players to the one recruiting one.

ID: Risk8

Name: Community Resources Scarce Availability

Resolution: Regular progress reporting and updating of plans. For what is concerned with the cost of these actions, no extra effort is needed besides the one dedicated to monitor the infrastructure operation.

ID: Risk9

Name: Requirements Poor Focus and Stability

Resolution: The involvement of the user communities in all the phases concurring to the delivery of the D4Science infrastructure will minimise such a risk. Moreover, the used Agile method combining top-down approach, functional design based on scenarios use cases, and the rapid prototyping in which users communities are continuously involved will guarantee that this risk be minimised. For what is concerned with the cost of these actions, they are in line with the standard requirement management activities.

ID: Risk10

Name: gCube Implementation Delays

Resolution: The project's work plan can tolerate minor delays between 1 and 3 months. Within these limits reassigning the focus of work teams and further prioritizing requirements can act as a countermeasure. Beyond this limit, delays of more than 3 months, requires severe reconsideration or strengthening of the team to which the work was initially assigned and could lead to effort reassignment if sufficient expertise is found outside the defaulting actor. In case of inability to re-assign work to a sufficient party, the resolutions include:

- Identifying expertise outside project's boundaries and summoning for external support;
- Selective drop-out of JRA activities.

For what is concerned with the cost of these actions, it can vary a lot, including the costs for hiring new stuffs, and lead to other risks. In particular, the drop-out of JRA activities

potentially may have a cascade effect impacting on the technology (gCube) as well as on the expected services (the infrastructure and the VREs).

ID: Risk11

Name: gCube Implementation Deviation

Resolution: The deviation is considered on a per-case basis. Furthermore the prioritization of the aspect where deviation is met is considered, allowing high priority incidents to be considered appropriately. The options for handling the risk are:

- Strengthening the implementation teams, when quality deviation stems from lack of resources or unforeseen need for extra implementation;
- Identifying and implementing workarounds for avoiding or minimising the risk to compromise requirements satisfaction;
- As a last resort, counterbalance failing activity by raising quality of other aspects of the system.

In case a component is not directly accessible but rather internally consumed, a workaround has to be crafted for the depending components, which have to either implement new facilities for overcoming the deviation, act on assumptions / lesser quality solutions, or even drop-out functionalities. For what is concerned with the cost of these actions, it can vary a lot, including the costs for hiring new stuffs or the design of alternative solutions. Moreover, these actions may result in other risks. In particular, the drop-out of functionality potentially may have a cascade effect impacting on the technology (gCube) as well as on the expected services (the infrastructure and the VREs).

ID: Risk12

Name: Community Data Deployment Deviation

Resolution: Seek alternate strategies to exploit the data; modify requirements to accept limited exploitation or abandon data source. For what is concerned with the cost of these actions, it can vary a lot, including the development of alternative approaches. Moreover, it can result in other risks like Community Low Uptake (Risk 7).

ID: Risk13

Name: Community Tools Deployment Deviation

Resolution: Seek alternate strategies to exploit the tool or provide similar features; modify requirements to accept limited exploitation or abandon the tool completely. For what is concerned with the cost of these actions, it can vary a lot, including the development of alternative solutions. Moreover, it can result in other risks like Community Low Uptake (Risk 7).

ID: Risk14

Name: Community Functionality Deployment Deviation

Resolution: Shift project resources; modify requirements to accept limited functionality or abandon the functionality completely. For what is concerned with the cost of these actions, it can vary a lot, including the development of surrogate solutions. Moreover, it can result in other risks like Community Low Uptake (Risk 7).

ID: Risk15

Name: gCube Release Availability Deviation

Resolution: Careful planning, monitoring and structuring of the integration activity by implementing continuous build and quick release cycles minimises the risk of delays in integrating the software delivered by JRA. Bugs, identified during the integration process, must be fixed with higher priority. For what is concerned with the cost of these actions, it is minimum even with a high number of integration cycles thanks to the

automation of this activity. Changes in priority of JRA development activity might result in other risks including gCube implementation delay (Risk 10) or deviation (Risk 11).

ID: Risk16

Name: gCube Release Poor Quality

Resolution: The released software is submitted to a validation team, before going to production, which executes a number of test cases based on NA5 and SA1 requirements. This can be done in the testing infrastructure. In alternative, these test cases can also be implemented in the SA3 test plan. For what is concerned with the cost of these actions, it is minimum because of the high automation level the test phase reached.

ID: Risk17

Name: gLite Node Low Availability

Resolution: Continuously monitor the status of the gLite nodes of the infrastructure. Follow the clear procedures defined by EGEE to deal with the unavailability of gLite nodes and bring the node as quickly as possible back in operation. For what is concerned with the cost of these actions, it is minimum because corresponds to the standard management of a distributed infrastructure and is supported by proper tools.

ID: Risk18

Name: gCube Node Low Availability

Resolution: Continuously monitor the status of the gCube nodes of the infrastructure. Strictly follow the D4Science support procedures to bring the gCube nodes back to operation whenever a problem is found. Restore the affected services in another node of the infrastructure if needed. For what is concerned with the cost of these actions, it is minimum because corresponds to the standard management of a distributed infrastructure and is supported by proper tools. Actually, it will grow if new hardware will be needed. The poor effectiveness in addressing this risk may result in other risks including the VRE operation deviation (Risk 21).

ID: Risk19

Name: Community Node Low Availability

Resolution: Continuously monitor the status of the community nodes of the infrastructure. Isolate the features associated with the services and data deployed in the community nodes in order to limit the impact of their unavailability. Duplicate the services and/or data on different domains, if possible. For what is concerned with the cost of these actions, it is minimum because corresponds to the standard management of a distributed infrastructure and is supported by proper tools.

ID: Risk20

Name: VREs Functionality Poor Effectiveness

Resolution: Define requirements and their relative importance early in project cycle so development team has adequate time to deliver critical functionality. Push (*i*) the developers in early prototyping the key functionalities and (*ii*) the infrastructure managers in making these services available for testing even if functionally incomplete or not in a production quality status. Inform the community on the known bugs and drawbacks. Early feedback on the released functionality must be provided to the developers. Ensure a close collaboration between NA, SA and JRA teams by periodic face-to-face meetings to keep this risk low. For what is concerned with the cost of these actions, it is minimum because it is not beyond the one needed to implement the project. The scarce effectiveness in addressing this risk may result in other risks including the Community Low Uptake (Risk 7).

ID: Risk21

Name: VREs Operation Deviation

Resolution: Ensure a close collaboration between SA and JRA teams by periodic face-to-face meetings where this risk is addressed and solutions discussed. JRA teams have to provide a higher level of support to the setup and operation of the VRE, in particular for the achievements of MSA1.2 and MSA1.3. For what is concerned with the cost of these actions, it is minimum because it is not beyond the one needed to implement the project. The scarce effectiveness in addressing this risk may result in other risks including the Community Low Uptake (Risk 7).

ID: Risk22

Name: VREs Availability Deviation

Resolution: Ensure a close collaboration between SA and NA teams by periodic face-to-face meetings where this risk is addressed and solutions discussed. For what is concerned with the cost of these actions, it is minimum (periodic phone conferences can be enough) because it is not beyond the one needed to implement the project. The scarce effectiveness in addressing this risk may result in other risks including the Community Low Uptake (Risk 7).

4.2.4 External Risks Resolution Procedures

ID: Risk23

Name: gCube Broken Dependency

Resolution: The JRA team that identifies the broken dependency notifies the rest of the implementation teams. It is not only a dependency problem that has to be reported when met, but also observation of "lazy" evolution of dependent components, which might be an indicator of future problems. Upon the identification of such issues the following actions should be taken:

- Identify the tolerance to potential drop-out of functionality / features upon the exclusion of the component;
- Identify the availability of similar components, giving a high preference to the open source market;
- Evaluate the cost/benefit of new development depending on the above-identified solutions.

Finally the decisions that can be taken, in decreasing preference order, are:

- Replace defaulting component;
- Implement new components capturing the expressed requirements;
- Drop-out functionality.

For what is concerned with the cost of these actions, it can vary a lot since they ranges from functionality drop out to alternative solutions implementation. Moreover, it may result in other risks including gCube implementation delay (Risk 10) or deviation (Risk 10).

ID: Risk24

Name: gLite Compatibility Issue

Resolution: The close collaboration between EGEE and D4Science guarantees that any problem can be anticipated and the risk minimised. For what is concerned with the cost of these actions, it corresponds to the effort needed to adapt existing software to the new gLite characteristics. The scarce effectiveness in addressing this risk can result in other risks including the gLite node low availability (Risk 17).

ID: Risk25

Name: ETICS Availability Issue

Resolution: The close collaboration between ETICS 2 and D4Science guarantees that any problem can be anticipated and the risk minimised. In the unlikely situation of inappropriateness of the ETICS system, one of the tools previously studied (by the DILIGENT project) to support the build and test activity of the gCube software, can be adopted. For what is concerned with the cost of these actions, it can vary a lot since the actions include the development of alternative solutions.

4.3 Risk Monitoring

The goal of the Monitoring is to observe the status of the risks and report on them. In order to properly support the Risk Management activity, the procedure and the tool implementing it (i) must be *flexible* enough to reflect the current status of the project activities with respect to the indicators to be observed; (ii) will support cooperation thus facilitating the production and discovery of the information needed to be informed on the project activities and their status; and (iii) open as to potentially serve any project member and provide a comprehensive picture of the project as a whole.

Because of the above motivations, a complex risk monitoring environment consisting of various web-based tools will be put in place:

- *a wiki page providing a comprehensive description of the identified risks*. For each risk the following information must be provided: a description, the situation under which the risk occurs, the "how-to" governing the risk management and the person that is responsible to monitor and handle it. This list identifies the risk factors the project consortium identified and for which management actions have been put in place. Whenever, unpredicted risks are recognised or envisaged, the list will be revised.
- *a wiki page reporting the top–n ranked risks*. This wiki page should continuously evolve because of the evolution of the factors that determine the risk rank. Each manager will take care to evaluate the risk exposure rank (each two weeks, i.e. the 1st and 15th of each month).
- *a wiki page containing the status of the occurred risks and the progress towards the resolution*. This web page will be edited per-risk by the Manager that is responsible for its management (cf. Section 4.1).
- *a shared workspace to support managers and task leaders in sharing data and information* (mainly Excel files) will be put in place. This shared work space will be mainly used to gather the input needed to produce the wiki page and keep them updated.
- a *monthly email on the status of this activity* will be sent to the PMB (the 20th of each month) from the Quality Assurance Task Force. The information contained in the email will be obtained by distilling the information contained in the risk monitoring environment.

5 CONCLUSIONS

Risks are combination of the probability of an event and its consequences. Any initiative, activity, organisation or undertaking is exposed to risks since in it there is the potential for events and consequences. D4Science does not escape this pattern and is exposed to a series of risks this report is about. In particular, this report presented the D4Science Risk Management approach, i.e. the structured and organised procedure put in place for risks treatment. Risk identification, evaluation, classification, planning, resolution and monitoring activities have been introduced and described. From these activities 25 major project risks have resulted. Each of these risks has been described including the identification of the event or activity the risk originates from, the project asset the risk impacts on and the corrective actions to put in place to nullify or mitigate its impact. These risks have been evaluated in order to recognise, among the identified risks, the major ones the D4Science consortium is exposed to. From this exercise resulted that the top risks (obtained by combining factors related to the value of the asset, the impact and the likelihood) are associated with (*i*) the delays in the implementation of the core components for the definition and operation of VREs, (*ii*) the deviation in providing the team guaranteeing the operation of the infrastructure and the related VREs with the latest technology enhancements, and (*iii*) the delays in producing technology enhancements. The rationale of having these technology-related risks as top ranked is well in line with the project mission, i.e. to provide user communities with an innovative e-Infrastructure supporting the operation of Virtual Research Environments a powerful and effective technology is the foundational mean to have.

GLOSSARY

Asset
Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.

Consequence
Outcome of an event. There can be more than one consequence from one event. Consequences can range from positive to negative. Consequences can be expressed qualitatively or quantitatively [4]

Event
Occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences. [4]

Evidence
Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.

Exposure
The potential loss to an area due to the occurrence of an adverse event.

Procedure
A written description of a course of action to be taken to perform a given task.

Process
An organised set of activities which uses resources to transform inputs to outputs.

Risk
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Risk Classification
Process to find, list and describe the elements of risk.

Risk Identification
Process to find, list and describe the elements of risk.

Risk Evaluation
Process of comparing risk characteristics to determine the significance of risk. Includes risk estimation process assigning values to the probability of a risk.

Risk Management
Process consisting of risk analysis (risk identification, risk evaluation and risk classification) and risk control (risk planning, risk resolution and risk monitoring).

Risk Monitoring
Process for measuring the status of risk.

Risk Object
A thing to which the specific risk is directed.

Risk Planning

Procedure and process regulating the management of the risk.

Risk Resolution

Process of selection and implementation of measures to modify risk. It can include risk avoiding, risk optimization, risk transferring and risk retaining approaches.

Risk Source

The event, activity, behaviours, item or body having the potential for a consequence, i.e. the risk originates from.

REFERENCES

[1] Andrade, P.; Candela, L.; Michel, J.; Pagano, P. *Quality Plan*. D4Science project Deliverable D1.2. April 2008

[2] Crockford, N. An Introduction to Risk Management. Woodhead-Faulkner. 0-85941-332-2. 1986

[3] Dorfman, M. S. Introduction to Risk Management and Insurance (9th Edition). Englewood Cliffs, N.J: Prentice Hall. ISBN 0-13-224227-3. 2007

[4] ISO/IEC Guide 73:2002 Risk management – Vocabulary.

[5] Stonebumer, G.; Goguen, A.; Feringa, A. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30. 2002