| | |
|---|---|
| Project acronym | D4Science-II |
| Project full title | Data infrastructure ecosystem for science |
| Project No | 239019 |

**Deliverable No DNA1.3**

# Risk Analysis and Risk Response

June 2010

**SEVENTH FRAMEWORK PROGRAMME**
**Research Infrastructures**

INFRA-2008-1.2.2: Scientific Data Infrastructures

# DOCUMENT INFORMATION

| | |
|---|---|
| Project | |
| Project acronym: | D4Science-II |
| Project full title: | Data Infrastructures Ecosystem for Science |
| Project start: | 1st October 2009 |
| Project duration: | 24 months |
| Call: | INFRA-2008-1.2.2: Scientific Data Infrastructures |
| Grant agreement no.: | 239019 |
| Document | |
| Deliverable number: | DNA1.3 |
| Deliverable title: | Risk Analysis and Risk Response |
| Contractual Date of Delivery: | June 2010 |
| Actual Date of Delivery: | 26 July 2010 |
| Editor(s): | P. Andrade |
| Author(s): | P. Andrade, L.Candela, G. Kakaletris, P. Pagano |
| Reviewer(s): | J. Klem |
| Participant(s): | ERCIM, CNR, NKUA, CERN |
| Work package no.: | NA1 |
| Work package title: | Project Management |
| Work package leader: | ERCIM |
| Work package participants: | ERCIM, CNR, NKUA, CERN, FAO |
| Est. Person-months: | 3 |
| Distribution: | Public |
| Nature: | Report |
| Version/Revision: | 1.1 |
| Draft/Final | Final |
| Total number of pages:<br>(including cover) | 16 |
| Keywords: | Risk Identification, Risk Evaluation, Risk Classification, Risk Plan, Risk Resolution, Risk Monitoring |

# CHANGE LOG

| Reason for change | Issue | Revision | Date |
|---|---|---|---|
| First version | 0 | 1 | 10/06/10 |
| Second version | 0 | 2 | 29/06/10 |
| Version for official review | 1 | 0 | 29/06/10 |
| Final version | 1 | 1 | 01/07/10 |
| | | | |

# DISCLAIMER

This document contains description of the D4Science and D4Science-II 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-ii.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-II 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-II is a project partially funded by the European Union**

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AFD | Administrative and Financial Director |
| BSCW | Basic Shared Collaborative Workspace |
| CERN | European Organization for Nuclear Research |
| CNR | Consiglio Nazionale della Ricerche (National Research Council) |
| D4Science-II | Data infrastructure ecosystem for science, an EC FP7 funded project |
| EAB | External Advisory Board |
| EC | European Commission |
| ERCIM | European Research Consortium for Informatics and Mathematics |
| EU | European Union |
| EUPL | European Union Public License |
| FAO | The Food and Agriculture Organization of the United Nations FAO |
| FP7 | Seventh Framework Programme of the European Community |
| JRA | Joint Research Activity |
| MGA | Members General Assembly |
| NA | Network Activity |
| NKUA | National and Kapodistrian University of Athens |
| PD | Project Director |
| PMB | Project Management Board |
| QATF | Quality Assurance Task Force |
| QR | Quarterly Report |
| SA | Service Activity |
| TB | Technical Board |
| TCOM | Technical Committee |
| TD | Technical Director |
| TMT | Technical Management Team |
| VO | Virtual Organization |
| VRE | Virtual Research Environment |

# TABLE OF CONTENTS

# LIST OF TABLES

# SUMMARY

This deliverable documents the methodology defined to identify, evaluate and classify the actual and potential risks the D4Science-II consortium and its related activities might be confronted with. In particular, the deliverable presents the adopted risk management methodology by detailing its different phases, procedures, tools, and actors involved. The deliverable relies on the procedures and experiences resulting from the D4Science project.

# EXECUTIVE SUMMARY

D4Science-II is a large-scale e-Infrastructure project involving multiple institutions with activities in areas as diverse as training and dissemination, deploying a production infrastructure, and addressing the technical requirements received by diverse scientific scenarios related to Fisheries and Aquaculture Resource Management, Biodiversity, Digital Libraries, and others.

To make sure the project objectives are met it is important to make sure that all activities are based on common objectives and that **risks** are avoided or clearly identified. Risks refer to the potential that a given threat will exploit vulnerabilities of a project asset and can consequently cause harm to the project. Since risks are factors that prevent the fulfilment of the project mission, countermeasures should be prepared.

To ensure that risks are properly handled, the project defined a Quality Assurance task (TNA1.2) responsible for the definition and monitoring of the project quality plan but also to work in the set up of a **risk management** methodology for the project. A risk management methodology is a set of methods and procedures used to identify both the risks the project is subject to as well as the actions to take in order to identify their happening and consequently react to minimise their effect.

The project risk management methodology consists of two main phases: the **risk analysis** and **risk control**. Each of them is composed by a number of steps.

The risk analysis phase 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 that the risk will have, the probability of occurrence, and the value of the assets;
- *Risk classification*: 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 risk control phase foresees three main steps:

- *Risk plan*: identifies the actors and the tasks required to control the risks in a common risk plan for the project;
- *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 to monitor the risks according to the priorities identified in the risk classification phase.

The goal of this deliverable is to present the methodology adopted in D4Science-II for risk management. This procedure is defined by relying on the procedure defined in the context of the D4Science project. The deliverable presents the different phases and steps composing the risk management methodology by defining the involved actors, procedures, and tools. Section 2 focuses on the risk analysis phase while Section 3 presents the risk control phase. The deliverable closes with a glossary of risk related terminology.

# 1 RISK ANALYSIS

## 1.1 Risk Identification Procedure

The first part of the risk analysis phase is about identifying and labelling the risks the project is exposed to. The identification of a risk is based on the usage of the terms source/problem and is further explained by the terms object/impact:

- 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.

**Who**

Because of their knowledge of the domain, work package leaders and project managers (in cooperation with tasks leaders when required) are the best candidates to identify possible risks affecting the activity of the project. Work package leaders identify low-level risks and their impact, while project managers identify high-level risks that are not directly conceivable at lower layers.

**How**

The main sources for identifying 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;
- As an initial indicator, the likelihood of appearance of the risk can also be attached.

The risk identification is a continuous task. When work package leaders or project managers decide to declare a new risk this should be done either immediately or, at the latest, during the preparation the next project Quarterly Report. If no risks are identified this should be communicated to the QATF when the Quarterly Report is produced. The QATF selected TRAC issue tracking system as the official tool to support the risk management activity. Therefore the declaration of new risks is carried out by creating a new ticket with type "risk" using the TRAC web interface available at:

https://issue.d4science-ii.research-infrastructures.eu/newticket

## 1.2 Risk Evaluation Procedure

Based on the findings of risk identification, all risks identified have to be evaluated.

**Who**

This step is carried out by work package leaders and project managers (in cooperation with tasks leaders when required).

**How**

The evaluation of a risk is performed by identifying the probability of occurrence and the impact for each risk. The probability for a particular source/problem to occur 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.

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-II case, this activity relies on "expert" opinions that evaluate the risks.

Moreover, the terms "probability rank" and "impact rank", which are more appropriate for the D4Science-II case, have been 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. The following table presents the convention defined for risk evaluation.

| **Probability Rank** | | **Impact Rank** | |
|---|---|---|---|
| **Description** | **Value** | **Description** | **Value** |
| Very Low | 1 | Doesn't affect the activity | 1 |
| Low | 2 | Affects the activity but a workaround is not needed | 2 |
| Medium | 3 | Affects the activity and it's recommended to put in place a workaround | 3 |
| High | 4 | Affects the activity and it's mandatory to put in place a workaround | 4 |
| Very High | 5 | Affects the activity that has to be completely rethought | 5 |
| Certain | 10 | Blocks the activity | 10 |

**Table 1 - Probability rank and impact rank**

The probability rank and impact rank information must be attached to all identified risks. Such values are declared in the TRAC ticket that represents the risk. The identification of these values is mandatory.

Work package leaders and project manager may also revise the probability rank and impact rank of risks already identified in the past. For such, they must update the corresponding TRAC ticket that represents the risk. This should happen at least once per quarter during the preparation of the project Quarterly Reports.

## 1.3 Risk Classification Procedure

Risk classification is the main task of the risk analysis phase. Having (1) the value of the asset associated to the risk, (2) the indicator of the probability of the risk being triggered, and (3)the impact this will have on the particular asset, it is possible to estimate the importance of the risk.

**Who**

This step is executed by the QATF after receiving the risk evaluation from work packages leaders and/or projects managers via the project Quarterly Reports.

**How**

The measurement of risks 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 |
|---|

The value of the asset can be defined as follows:

- All assets that do not depend on other assets
    - Value of asset = 1;
- All assets that depend on other assets
    - Value of asset = C-Value
    - C-Value = K * Value of lower level asset (K <= 1; e.g. K = 0.9 and so on to reduce the value of the assets that depend on a chain of 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.

In D4Science-II the sorting is primarily done using the risk exposure rank. The sorting by probability will only be used as a secondary option.

This calculation of the risk exposure rank is done by the QATF when a new risk is added to the risks plan or when the probability rank and/or impact rank of an existing risk is updated. At the most the risk exposure rank for all risks should be verified every three months when the project Quarterly Reports are approved.

Such operation is carried out by updating the risk exposure rank filed present in the TRAC tickets representing the affected risks. After updating the risk exposure rank, all existing risks are automatically re-sorted by TRAC reporting facilities. The sorted risk rank is available at:

https://issue.d4science-ii.research-infrastructures.eu/report/36

# 2 RISK CONTROL

## 2.1 Risk Planning Procedure

The risk control phase operates on an enriched set of information already gathered as part of risk analysis. This information is assembled during the risk planning step and leads to the creation of a risk plan.

### Who

This step is a shared responsibility between the QATF, work packages leaders, and project managers.

### How

The risk plan contains all risks identified by the risk classification step of the risk analysis phase. In particular, the top-ranked risks must contain the following information:

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

Besides the definition of the risk plan itself it is also important to:

- Set responsibilities for managing the plan itself;
- Perform periodical updates of the plan;

The QATF must ensure that all top-ranked risks are fully described. When a risk is considered as top-ranked, the QATF asks the relevant work package leader and/or project manager to add the information described above (how to monitor the risk, risk countermeasure, responsible for monitoring that risks, etc) to the risk ticket in TRAC. This activity is carried out at least every three months when the project Quarterly Reports are approved.

The top-ranked risks are highlighted in the risk plan report available in TRAC: https://issue.d4science-ii.research-infrastructures.eu/report/36

## 2.2 Risk Monitoring Procedure

The most effective way of monitoring risks is the continuous update of the top-ranked risks as defined in the risk plan. Among the top-ranked risks it is important to implement the actions of 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 is also maintained:

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

### Who

The monitoring of project risks is responsibility of work packages leaders, project managers, and the PMB.

### How

The risk monitoring is a continuous task. However it is mandatory to follow the risk plan status every time the QAFT re-sorts the existing risks to understand which risks are now top-ranked and require therefore close monitoring.

If a risk increases its exposure rank, the projects managers should introduce more accurate countermeasures and inform the PMB to allow a high-level discussion. Similarly but with the reverse impact, risks that gradually diminish, have their countermeasures relaxed. The impact of these tasks should then be documented in the next Quarterly Report so that the risk can be re-classified and re-sorted.

## 2.3 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 the probability of its triggering events;
- Avoid the risk by removing its connection with project activities;
- Transfer the danger to another party or asset to reduce the probability of occurrence;
- 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 of limiting the effects on the project.

**Who**

The risk resolution is a responsibility of work packages leaders and project managers.

**How**

Risks are resolved by applying the actions defined in the risk plan for each risk. These actions must be executed when a risk is sorted by the QATF as a top-ranked risk.

# GLOSSARY

### Asset

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

### 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.

### 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 Identification

Process to find and list 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 and impact of a risk.

### Risk Classification

Process to sort risks based on a pre-defined criteria.

### 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, behaviour, item or body having the potential for a consequence, i.e. the risk originates from.

# REFERENCES

[1] Andrade, P.; Candela L.; Faggian Marque, Roberta; Michel, J.; Pagano, P. Risk Analysis and Risk Response. D4Science Project Deliverable, DNA1.3a August, 2008

[2] Candela, L.; Pagano, P. Risk Analysis and Risk Response. D4Science Project Deliverable, DNA1.3b August, 2009

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