Risk Assessment in Open Source Systems

Xavier Franch
Group of Software and Service Engineering
Universitat Politècnica de Catalunya
Barcelona, Spain
+34 - 93 413 7891
franch@essi.upc.edu

Angelo Susi
Software Engineering Unit
Fondazione Bruno Kessler (FBK)
Trento, Italy
+39 0461 314344
susi@fbk.eu

ABSTRACT
Adopting Open Source Software (OSS) components offers many advantages to organizations but also introduces risks related to the intrinsic fluidity of the OSS development projects. Choosing the right components is a critical decision, as it could contribute to the success of any adoption process. Making the right decision requires to evaluate the technical capabilities of the components and also related strategic aspects, including possible impacts on high level objectives. This can be achieved through a portfolio of risk assessment and mitigation methods. In this briefing we introduce the basic concepts related to OSS ecosystems and to risk representation and reasoning. We illustrate how risk management activities in OSS can benefit from the large amount of data available from OSS repositories and how they can be connected to business goals for strategic decision-making. The concepts are illustrated with a software platform developed in the context of the EU FP7 project RISCOSS.

CCS Concepts
• **Software and its engineering→Software notations and tools**

Keywords
Risk assessment; Open Source Software; Conceptual modelling.

1. MOTIVATION AND OBJECTIVES
In 2016 an estimated 95% of all commercial software packages will include OSS [1]. The intrinsic properties of OSS require substantial changes in the company-internal component evaluation processes exposing them to several risks [2]. OSS projects are developed in open and distributed development communities, guided by heterogeneous personal and business objectives, and provided without quality of service agreements or formal commitments on the future roadmap. In this setting, risk assessment can benefit from the open nature of the OSS ecosystems [3]. In fact, a large amount of data is available in software repositories and community-related artefacts, describing several aspects of the OSS ecosystems.

ICSE '16 Companion, May 14-22, 2016, Austin, TX, USA
ACM 978-1-4503-4205-6/16/05.
http://dx.doi.org/10.1145/2889160.2891052

For example, data are referred to the behavior of the communities in terms of their commitment to the OSS project or their cohesion and capacity to attract new members. Other data may refer to the maturity and characteristics of the components and of their robustness.

A risk management framework acting on OSS projects may take advantage of these data. For example, the framework can be structured around different levels of analysis where a bottom layer may gather data both from communities and projects. This data can be aggregated in an intermediate layer to populate a set of risk indicators variables that describes the exposure to a given risk due the values gathered in the previous layer. These risk indicators can be then analyzed in order to establish the impact of the risk on business goals.

The overall goal of the technical briefing is that of having an overview of the state of the art and future directions in risk analysis in the scenario of OSS adoption. The briefing focuses on the modeling of, and reasoning on, risks arising in a typical decision-making activity related to software development process. It also gives a view on how this decision affects both the business and software ecosystems of a given organization. This can open several interesting research challenges that go from the introduction of new concepts in the existing modeling framework to represent peculiarities of the OSS ecosystems, to the possibility of developing new reasoning techniques suited for this particular domain. This goal is broken into the following objectives.

- Introducing the concept of OSS ecosystem [4].
- Introducing the concepts of risk, risk assessment and mitigation, in general [5] and specifically for OSS ecosystems [2][3].
- Introducing a portfolio of modelling and analysis techniques for risk assessment in the context of OSS ecosystems [6][7][8].
- Introducing the risk analysis process [3].
- Introducing the different capabilities of a risk analysis supporting platform [9].

The briefing considers the results of an EU project called RISCOSS (www.riscoss.eu) that has developed a software platform that implements this 3-layer view. The risk models in the project (about licenses, security, ...) have been build from the knowledge gathered by partners of different kind, like Ericsson (big corporation), OW2 (OSS foundation) and CENATIC (Spanish public observatory)

The briefing is addressed to a wide audience. For researchers, an updated state of the art will be exposed, a particular approach will be explored in depth, and the presentation will rely on scientific grounds. For OSS contributors, risk management will provide an additional perspective to manage OSS projects. For educators, the briefing will provide the basis for developing course material.

2. BACKGROUND

The briefing will rely in a textbook for risk management as background [5]. A set of scientific papers produced in the RISCOSS project serve to document the main concepts presented [3][6][7][8]. As for tool support, during the briefing we use the RISCOSS platform [9]. The current version of the platform can be accessed at https://github.com/RISCOSS/riscoss-corporate. This open source tool is made available during the briefing for some short hands-on exercises to assess the level of risk (on licenses, security, etc.) in OSS projects according to some risk models. Mitigation actions are also explored and evaluated.

3. CONTENTS

The technical briefing is organized with a structure that matches the objectives identified above. It is organized in four parts aiming at introducing the theoretical and methodological aspects and processes related to risk identification and analysis in OSS adoption. We start with an introductive parts whose main purpose is that of describing a motivating example and the related risks and organizational concepts. We then introduce the main risk factors in OSS giving a background on OSS ecosystems, presenting an analysis of the risk factors and an example of OSS adoption related risks. The RISCOSS approach is then introduced in order to link the theoretical aspects with a concrete methodology and supporting platform. We conclude summarizing and discussing the main achievements. We present below some details of these topics below (except for motivation already introduced in Section 1).

3.1 Risk Related Concepts

In order to effectively manage and control risk, management needs a clear and detailed picture of the risk and of the environment in which they occur. Without this knowledge, appropriate actions cannot be taken to deal with rising problems. For this purpose, risks must be identified, this includes the risk sources, the risk events and the risk consequences, and mitigated. To allow the description of these aspects several risk ontologies have been proposed that introduces concepts such as those of measures, risk indicators, risk events and mitigation activities. These concepts are then connected to the concepts related to the description of the OSS ecosystems and of the OSS adopting organizations such as those of goals, activities or resources in order to represent the impact of risks on the organizational assets. The concepts and relationships defined so far allow to encode the experts' knowledge into (visual) risk and organizational models.

3.2 The Risk Analysis Approach

An important aspect of the risk analysis in OSS adoption is the capacity to exploit data from the OSS projects and communities to evaluate the exposure to risks and the impact on the goals of the adopting organization. In the approach proposed in RISCOSS [3] the analysis is based on a three layered view to risk management in OSS.

- In Layer I the available data and measures from OSS communities and project are gathered and aggregated to have the representation of the state of the OSS ecosystem. Qualitative information coming from domain experts may be used to elicit the context of adoption.
- In Layer II the data from Layer I are used to populate a set of risk indicators that, for example, reports on the behavior of a give community in terms of timeliness or activeness.
- In Layer III the data from the indicators are used to establish the exposure to risks and the impact a particular risk has on the goals, or activities of an OSS adopter organization.

3.3 The Risk Assessment Platform

In our case, the risk assessment approach is supported by the RISCOSS decision-making platform. It has been developed thanks to the collaboration of academic institutions, companies and OSS communities. The platform allows the specification of the organizational assets, the knowledge related to the risks and organization in terms of models and allows to calculate, through statistical and logic based techniques, the exposure to risks and the impacts on the organizational assets.

4. CONCLUSIONS

This technical briefing aims at providing an overview of the risks in OSS adoption and of the conceptual frameworks and reasoning techniques set up to deal with this problem. The exemplar method described during the briefing not only intends to cope with OSS technical related risks but it also highlights the importance of identifying the impact of these risks on the strategy and assets of the OSS adopting organization and on the other actors in the OSS ecosystem for an holistic risk management and mitigation.

5. PRESENTERS

Xavier Franch is Associate Professor at UPC, Spain. He is the leader of the research group on Software and Service Engineering (GESSI). He is the project manager of the RISCOSS FP7 EU project which is highly related to the topic of this briefing.

Angelo Susi is a research scientist in the Software Engineering group at Fondazione Bruno Kessler in Trento, Italy. His research interests are in the area of requirements engineering, He is the scientific manager of the RISCOSS FP7 EU project.

6. ACKNOWLEDGMENT

This work is a result of the RISCOSS project, funded by the EC 7th Framework Programme FP7/2007-2013 under the agreement number 318249.

7. REFERENCES

[1] M. Driver. "Drivers and Incentives for the Wide Adoption of Open- Source Software", Gartner Report, Sept. 13, 2012.

[2] X. Franch et al. "Managing Risk in Open Source Software Adoption". ICSOFT 2013: 258-264.

[3] X. Franch, R. Kenett, A. Susi, N. Galanis, R. Glott, F. Mancinelli. "Community Data for OSS Adoption Risk Management". In *The Art and Science of Analyzing Software Data*, C. Bird, T. Menzies, T. Zimmermann (eds.), John Wiley & Sons, , Inc., Hoboken, NJ, 2015.

[4] S. Jansen. "Measuring the Health of Open Source Software Ecosystems: Beyond the Scope of Project Health". IST 56, 2014: 1508-1519.

[5] Y.Y. Haimes, *Risk Modelling, Assessment and Management*, 3rd Edition, John Wiley & Sons, Inc., Hoboken, NJ, 2009.

[6] A. Siena, M. Morandini, A. Susi. "Modelling Risks in Open Source Software Component Selection". ER 2014: 335-348.

[7] D. Costal, L. López, M. Morandini, A. Siena, M.C. Annosi, D. Gross, L. Méndez, X. Franch, A. Susi. "Aligning Business Goals and Risks in OSS Adoption". ER 2015: 35-49.

[8] P. Giorgini, J. Mylopoulos, E. Nicchiarelli, R. Sebastiani. "Formal reasoning techniques for goal models". J. Data Semantics, 1, 2003: 1–20.

[9] X. Franch et al. "The RISCOSS Platform for Risk Management in Open Source Software Adoption". OSS 2015: 124-133.