Managing Risk in Open Source Software Adoption

Xavier Franch[1], Angelo Susi[2], Maria C. Annosi[3], Claudia Ayala[1], Ruediger Glott[4], Daniel Gross[2], Ron Kenett[5], Fabio Mancinelli[8], Pop Ramsamy[7] and Cedric Thomas[6], David Ameller[1], Stijn Bannier[4], Nili Bergida[5], Yehuda Blumenfeld[5], Olivier Bouzereau[6], Dolors Costal[1], Manuel Domínguez[7], Kirsten Haaland[4], Lidia López[1], Mirko Morandini[2], Alberto Siena[2]

[1]*Universitat Politècnica de Catalunya (UPC), Spain;* [2]*Fondazione Bruno Kessler (FBK), Italy;* [3]*Ericsson Telecomunicazioni, Italy;* [4]*University of Maastricht (UMM), The Netherlands;* [5]*KPA Ltd., Israel;* [6]*OW2, France;* [7]*CENATIC, Spain;* [8]*XWiki SAS, France*

{franch,dameller,cayala,dolors,llopez}@essi.upc.edu {susi,gross18,morandini,siena}@fbk.eu, mariacarmela.annosi @ericsson.com, {stijn.bannier,glott.ruediger,kirstenhaaland}@gmail.com, {nilib,yehudab,ron}@kpa-group.com, {olivier.bouzereau,cedric.thomas}@ow2.org, {manuel.dominguez,pop.ramsamy}@cenatic.es, fabio.mancinelli@xwiki.com

Keywords: Open-Source Software, OSS, Risk Management, Software Ecosystem, Strategic Modelling, iStar.

Abstract: By 2016 an estimated 95% of all commercial software packages will include Open Source Software (OSS). This extended adoption is yet not avoiding failure rates in OSS projects to be as high as 50%. Inadequate risk management has been identified among the top mistakes to avoid when implementing OSS-based solutions. Understanding, managing and mitigating OSS adoption risks is therefore crucial to avoid potentially significant adverse impact on the business. In this position paper we portray a short report of work in progress on risk management in OSS adoption processes. We present a risk-aware technical decision-making management platform integrated in a business-oriented decision-making framework, which together support placing technical OSS adoption decisions into organizational, business strategy as well as the broader OSS community context. The platform will be validated against a collection of use cases coming from different types of organizations: big companies, SMEs, public administration, consolidated OSS communities and emergent small OSS products.

1 INTRODUCTION

Open Source Software (OSS) has become a strategic asset for a number of reasons, such as its short time-to-market software service and product delivery, reduced development and maintenance costs, and its customization capabilities. Open source technologies are currently embedded in almost all commercial software – by 2016, they will be included in 95% of all commercial software packages (Gartner, September 2012).

In spite of the increasing strategic importance of OSS technologies, still IT companies and organizations face numerous difficulties and challenges when making the strategic move to the open source way of working. In fact, according to the most popular OSS portal, SourceForge, most OSS projects have ended in failure: 58% do not move beyond the alpha developmental stage (22% of them remain in the planning phase, while 17% remain in the pre-alpha phase, and some of them become inactive). Among the roots for these failures, it stands that OSS is about freedom and choice, but freedom and choice introduce risk (Gartner, June 2011). The risks that IT companies face when integrating OSS components into their solutions are not to be neglected and incorrect decisions may lead to expensive failures. Insufficient risk management has been recently reported as one of the five topmost mistakes to avoid when implementing OSS-based solutions (Gartner, November 2011). Financial institutions are required to manage such risks under the Basel III global regulatory standard and their capital requirements are determined accoridingly (Kenett and Raanan, 2010). With proper risk management and mitigation, failure could be reduced or negative impact and cost minimized.

In this position paper, we portray a short report of our work in progress in the RISCOSS European

project, that focuses on risk management in OSS adoption. Our framework will provide tools and methods for community-based OSS development, composition and life cycle management for practicing an effective management of OSS integration related risks and controlling and reducing the costs derived from the adoption of OSS. The rest of the paper is organized as follows. Section 2 provides more details on risks for OSS projects. Section 3 gives a short description of the background about the concept of ecosystems; Section 4 sketches he proposed framework. Section 5 discusses some research challenges. In Section 6 some principles for the validation of the framework are given. Section 7 concludes the paper.

2 RISKS IN OSS PROJECTS

To take maximum advantage of OSS adoption, the understanding and management of all the risks becomes necessary since they directly influence business, with strong effects on business models, e.g. concerning the production of OSS in business ecosystems, customer relations and customer satisfaction, cost structures and revenues. In addition, OSS and the possible involvement of "non-commercial" actors (such as OSS communities) in business processes bear also a potentially strong impact on brand image and time-to-market, thus on business strategies that underlie business models (Soto & Ciolkowski 2009). Evidently, a business model that offers value propositions based on OSS but not supported by an OSS-related business strategy, is likely to fail because business risks deriving from OSS will be overlooked.

Technical risks related to OSS can be manifold and might include evaluation, integration, context, process, quality and evolution risks. Empirical studies (Li et al., 2008) show in particular that the underestimation of integration efforts is one of the most challenging problems still requiring further investigation. The risk management strategy is always a problem that needs to be taken care of throughout the whole lifetime of OSS-based solutions, and is even more valuable during their maintenance phase. This takes into consideration the fact that the cost of maintenance is high, because maintenance is a time-consuming activity. Moreover, OSS-based solutions are not developed and do not exist in isolation. Instead, they exist in the wider context of an organization or a community, in larger OSS-based software and business ecosystems, which include groups of projects that are developed and co-evolve within the same environment but also further beyond their context, including the organization itself, OSS communities, regulatory bodies, etc.

A typical OSS scenario is as follows. An IT organization produces a product family for a particular domain. For each product within the product family, the organization keeps always two different release versions (the current and the previous one) and a third one under development. Moreover, each of these versions may require adaptation for different customers, e.g. due to regional laws, yielding thus to more and more variants. Each of these resulting variants is typically composed by a long list of third-party products, many of them OSS components, potentially different (for versions, patch level, etc.) from each other and with dependencies among them. Altogether, the organization is managing a complex software and business ecosystem where several questions emerge, e.g.: *(i)* how to design the possible viewpoints from which one can look at an ecosystem in order to collect relevant information for managing the evolution for the OSS products embedded in the products? *(ii)* how to secure that specific features of OSS do not harm business models and their underlying business strategies? *(iii)* how to implement a systematic approach towards understanding and representing dependencies involving OSS components for assessing risks?

The answer to these and similar questions requires the clear understanding of OSS-based ecosystems from a strategic perspective, with clear identification of relevant strategic dependencies (not just software dependencies) in order to control and mitigate all the risks coming from the adoption of OSS components along the lifetime of the different products being part of the ecosystems. Approaches (such as Software Sustainability Maturity Model, by OpenDirective; and OSS Watch and Reuse Readiness Levels, by NASA (RRL, 2013)), propose methods to assess the maturity of the software to be adopted.

3 BUSINESS AND SOFTWARE ECOSYSTEMS

Our approach basically elaborates around the idea of business and software ecosystems.

Moore (1993) coined the term *business ecosystem* to describe: "an economic community supported by a foundation of interacting

organizations and individuals—the organisms of the business world. This economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organizations also include suppliers, lead producers, competitors, and other stakeholders. Over time, they co-evolve their capabilities and roles, and tend to align themselves with the directions set by one or more central companies. Those companies holding leadership roles may change over time, but the function of ecosystem leader is valued by the community because it enables members to move toward shared visions to align their investments and to find mutually supportive roles".

Business ecosystems have their equivalent at the technological level. Messerschmitt and Szyperski (2003) used the term *software ecosystem* to describe the broader commercial, legal (regulatory) and market context in which traditional software systems operate. Companies such as Apple and Google have embraced a network centric view of software ecosystems, and developed novel business models, with varying degrees of openness – from the adoption of selected open web standards, to the promotion of key web APIs as ad-hoc standards, to the (more or less) full embrace of open source software – to encourage the emergence of massive global hardware/software ecosystems surrounding their products and services (e.g. iPhone, Android, etc.). Key arguments why companies adopt a software ecosystem approach to support their products and services offerings include (Bosch, 2009, Qualypso 2013): increase value of the core offering to existing users; increase attractiveness for new users; accelerate innovation through open innovation in the ecosystem; collaborate with partners in the ecosystem to share cost of innovation; "platformize" functionality developed by partners in the ecosystem (once success has been proven), and decrease total cost of ownership for commoditizing functionality by sharing the maintenance with ecosystem partners.

When it comes to OSS, both types of ecosystems have their peculiarities. As mentioned before, OSS-based business ecosystems require business models that take account of the potential impact of OSS specifics on the production, distribution, costs and revenues aligned with or derived from OSS-related value propositions. OSS-based software ecosystems should address licensing problems, component interdependencies and frequency of releases, for instance. Helander & Rissanen (2005) focus on the co-creation of value in OSS value networks, thus highlighting an aspect of OSS-based ecosystems that is important especially for businesses. The authors define value-creating networks "...as entities consisting of several directly or indirectly connected individual or organizational actors that transform and transfer different kinds of resources in order to create value not only for the network's end customer but also to themselves." Each actor within the value network performs those tasks in which he has specific expertise, and together all partners create added value that finally benefits the end user. There are a number of diverse actors that can form an OSS value network, starting from OSS projects and developer communities and ending with various end users, and mediators in between. Each actor is assumed to pursue common as well as particular interests.

The links between more strategic business ecosystems and more IT-oriented software ecosystems is one of the focal points of our approach.

4 THE FRAMEWORK

The framework elaborates on the concept of OSS value networks (Helander & Rissanen, 2005). It is supported by a collaborative platform that provides the entry-point for describing, analysing and performing decisions in OSS business and software ecosystems. The platform is composed of two tiers, the decisional tier that provides assessment to companies, and the technological tier that embeds the software system and provides observations to the decisional tier for decision-making. The company products integrate components coming from OSS communities or enterprises, whose adoption may require a negotiation between the community and the interested company. This negotiation is undertaken under perceptions of a shared conceptualization that can be different (for example organisations having a strong business orientation, and small OSS communities that do not consider business as an objective), hampering the understanding among the parties.

At this point several questions arise around the notion of ecosystem: How do the two tiers align? Which form takes the (highly strategic) decisional tier model? Which techniques can be applied for effective decision-making in the decisional tier? Which business processes and services can be established around the OSS business ecosystem? What form assumes the shared conceptualization? In the next section, we briefly analyse these open questions and provide first steps for their answer

5 RESEARCH CHALLENGES

We envisage the need to define: precise ontologies for OSS risks, to represent the common and shared set of concepts related to software and business ecosystems; risk modelling methods and notations; formal and statistical analysis techniques for risk assessment and mitigation; and mitigation strategies. In the following we analyse some of these aspects.

5.1 OSS Ontologies

An important characteristic of the proposed framework is a shared conceptualization of the OSS domain between communities and organisations (such as companies or public administration) in the ecosystem. We propose the use of a foundational ontology as conceptual tool for representing fundamental concepts in business and (open source) software ecosystems. Relevant for the ontology are the concepts describing the business and technological tiers and their relationships. These concepts may be added on top of existing foundational ontologies such as DOLCE (Gangemi et al., 2003) or UFO (Guizzardi and Wagner, 2005). To that end, it is necessary to use some ontology engineeering method like Methontology (Fernández-López et al., 1997), principles for evaluation as Grüber's (Grüber, 1995) and adequate tool support (e.g., Protegé). The concepts and relationships in the ontology will feed the process of development of a specific modelling notation for the ecosystem representation, which at its turn should be assessed not just in terms of expressiveness but also ease of use by modellers, e.g. evaluating Moody's principles for graphical notations (Moody, 2009).

5.2 Ecosystem Modelling

Strategic modelling and analysis of OSS-based ecosystems is a key asset for the proposed framework and calls for a comprehensive representation of the elements of OSS-based ecosystems (such as projects, communities, stakeholders, norms, licenses, risk) and analysis techniques to discover relevant properties of these ecosystems with the aim of reusing it in designing new and more efficient ecosystems.

Candidate techniques for ecosystem modelling and analysis are the actor / goal-oriented methodologies, such as *i**/Tropos (Yu, 95), and business process representation and reasoning methods. Over the last decade, in fact, a number of goal- and actor-oriented modelling and analysis techniques have been proposed to specifically assist in dealing with stakeholder motivation, interests and needs during the construction of a software system. Goal-oriented techniques allow the modelling of the strategic, social, synergistic or conflicting dependencies between the actors. The methodologies also allow the representation of the rational of each one of the actors participating in the ecosystem. This representation is performed in terms of the goals of the actor, the activities to be performed for the goal achievement, the resources available to the actors for the execution of the activities and dependencies between the actors for goal achievement. Moreover, goals can be AND/OR decomposed into sub-goals, allowing for the representation of alternative strategies to accomplish a given goal, so opening to the possibility of representing and reasoning about different possible ecosystem configurations. To complement these methods, business risk analysis and business process modelling techniques can be exploited to represent and reason on the processes performed in the organizations in the ecosystems to achieve the goals specified in the goal modelling (Giorgini et al., 2003; Kenett and Raanan, 2010). Finally, the aspect of the analysis of the ecosystem models could rely on formal and/or statistical techniques (see, for example, van Lamsweerde and Letier, 2000) and on new search based techniques.

5.3 Risk Management

An important aspect of the decisional tier of the envisaged framework is risk management. To tackle this problem, decision processes and techniques customized to this aspect need to be developed. These techniques are expected to exploit the data from the technological tier and from the business perspective to support risks and costs decision-making in the organization allowing for the identification of potential hidden risks tied to the different ecosystems and to validate early mitigation techniques. Next to qualitative and quantitative business economics methods, both advanced software engineering techniques and statistical approaches are seen as valuable for the framework. Advanced SE techniques include conceptual modelling and analysis approaches (Asnar et al., 2011), search-based software engineering techniques, such as multi-criteria genetic algorithms (Deb et al., 2002), as well as the more formal satisfiability modulo theories (Palma et al., 2011). Statistical approaches rely on logical regression,

value at risk assessment, as well as Bayesian Networks, multivariate scoring methods and association rules (Kenett & Raanan, 2010). We think it is important to distinguishing among lightweight assessment techniques for small businesses and in-depth measurement and optimization techniques applicable in large enterprise organizations and communities. Both modalities should be available and easy to customize.

5.4 Business Risk Analysis for OSS

Every business is based on objectives such as value creation and revenues. Business models capture the ways the organization intends to achieve them. Therefore, there is no enterprise without a business model (being it explicit or implicit) (Teece, 2010). Underlying business models are business strategies that translate the overall economic goals of an enterprise into values, actions and priorities etc. (Osterwalder et al., 2005).

Many of the OSS business model types do not necessarily rely on OSS – they would also work with proprietary software. What is currently lacking is a systematic identification of the OSS specific impact on business model components, business strategies, features, processes, opportunities and risks.

In this area, the objective of the framework is the integration of generic and OSS-specific business risk assessment approaches, tools and methods. These methods should allow for modelling business risks that affect community based and industry supported OSS development, composition and life cycle management and develop methods and tools to mitigate these risks. Moreover, since a business model is always a unique object suiting exactly one company and because business models have to adapt to environmental changes over time, typical business risks should be evaluated with regard to typical risks at the level of business model components and within the business ecosystem context. Such business model components are, for instance, the value proposition(s), the partners needed to produce a value proposition, the resources needed to create a value proposition, the activities that must be performed in order to produce a value proposition, the customer segments, the relations to the customers, the channels (for communication, distribution and sales), the costs and the revenues.

In fact, for example, a company should be aware of its dependence on an OSS developer community in order to assess the business risk that it provides for its business in a holistic way.

6 A VALIDATION PLAN

We aim at validating the framework via a scenario-based approach. To this end we need to define a comprehensive validation plan considering several dimensions: *Role* (producer, consumer, community), *Setting* (industrial, academia, public administration), *Size* (large, medium, small organizations), *Business strategy* (from full OSS collaboration to OSS exploitation), *Business process* (adoption, migration, consolidation, improvement).

Each data point determined by these dimensions provides a different scenario. For instance, a large industrial consumer may be interested in consolidating its current approaches that aim at producing highly reliable products in a structured software product line without getting too much involved in OSS communities and with only little interest to change processes. Here the tension may be between the need to reduce the time-to-market of a given product and the need of evaluating possible risks that can emerge from the adoption of components managed by communities that are not committed in assuring continuity in the components maintenance. In the case of small industrial consumers, consolidation may be targeted by entering into OSS ecosystems as a means to increase the availability of components and knowledge to be used in their products and a means to deliver their own products in the OSS ecosystem in order to create opportunities for new kinds of business. Also in this case one risk is that of having crucial components no more maintained by the community, so inducing the need to reconfigure the structure of the products and of the entire company business. For large (e.g., national-wide) public administration consumers, OSS adoption could result in decreasing the organisational costs. In this case, the tension is between low purchasing costs of OSS but possibly underestimated costs for building up the capacities to maintain and adapt these components in an effective way over time also monitoring the OSS ecosystems behaviours.

7 CONCLUSIONS

This position paper described opportunities and issues an organisation has to face with when it decides to adopt Open Source Software. It is a short report of work in progress that is part of a European project involving 8 partners. We focused on the aspect of OSS adoption risks, envisaging the

characteristics of a methodology, and the related supporting platform, to help the organizations in evaluating and mitigating these kinds of risks.

An important property of the proposed approach is that it considers the adoption risks problem in a holistic way, meaning that it does not only focus on the technical properties of the OSS components that have to be introduced in the organization, but also evaluates the impact this introduction has on the strategic and business level of the organisation and of the entire ecosystem the organisation belongs to. We believe that, in the case of OSS more than in the case of proprietary components and/or tools, the ecosystem and community dimensions are crucial to assess and mitigate the risks related to the adoption because, for example, the production and distribution of software in OSS follows different rules and values than pure commercial and competitive interests. Moreover, the dependency that OSS components naturally establish between the organisation and the OSS communities influences the business strategies of the organisation, for example reducing the time-to-market for particular products or increasing the variability in the product line of the organisation because of the variety of the components available from the communities.

Acknowledgements

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

REFERENCES

Asnar Y., Giorgini P., Mylopoulos J., 2011. "Goal-driven risk assessment in requirements engineering". *Requirements Engineering* 16(2), 101-116.

Bosch, J., 2009. From Software Product Lines to Software Ecosystems. In SPLC'09, 13th International Software Product Line Conference. ACM.

Deb, K., Pratap, A., Agarwal, S., Meyarivan, T., 2002, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Trans. On Evolutionary Computation*, ,vol.6, no.2, pp.182-197.

Fernández-López, M. Gómez-Pérez, A. Juristo, J., 1997. "METHONTOLOGY: From Ontological Art Towards Ontological Engineering". In Ontological Engineering AAAI-97 Spring Symposium Series.

Gangemi, A., Guarino, N, Masolo, C., Oltramari, A, 2003, "Sweetening WORDNET with DOLCE". 13-24 24 AI Magazine 3.

Gartner Group, September 2012. Understand the Challenge of Open-Source Software. Gartner Reports.

Gartner Group, June 2011. Critical Strategies to Manage Risk and Maximize Business Value of Open Source in the Enterprise. Gartner Reports.

Gartner Group, Novembre 2011. Five Mistakes to avoid when Implementing Open-Source Software. Gartner Reports.

Grüber, T.R., 1995. "Towards Principles for the Design of Ontologies used for Knowledge Sharing". Int. Journal on Human Computer Studies, 43, 907-928.

Giorgini P., Mylopoulos J., Nicchiarelli E., Sebastiani R., 2003. "Formal Reasoning Techniques for Goal Models". LNCS (2800), 1-20.

Guizzardi, G., Wagner, G., 2005. "Some Applications of a Unified Foundational Ontology in Business Modeling". Business Systems Analysis with Ontologies, IGI Global, 345-367.

Helander, N., Rissanen, T., 2005. Value-Creating Networks Approach to Open Source Software Business Models. *Frontiers of E-Business Research*.

Kenett, R., Raanan, Y., 2010. *Operational Risk Management: A Practical Approach to Intelligent Data Analysis*. John Wiley & Sons.

van Lamsweerde, A. Letier, E., 2000. "Handling Obstacles in Goal-Oriented Requirements Engineering". 978-1005 2000 26 *IEEE Trans. Software Eng.* 10

Li, J., Conradi, R., Slyngstad, O.P.N., Torchiano, M., Morisio, M., Bunse, C., 2008. A State-of-the-Practice Survey of Risk Management in Development with Off-the-Shelf Software Components. *IEEE Trans. on Software Eng.*, 34(2).

Messerschmitt, D.G., Szyperski, C., 2003. *Software Ecosystem: Understanding an Indispensable Technology and Industry*. The MIT Press, Cambridge, Mass.

Moody, D.L., 2009. "The "Physics" of Notations: Toward a Scientific Basis for Constructing Visual Notations in Software Engineering". *IEEE Trans. Software Eng.* 35(6): 756-779.

Moore, J.F., 1993. Predators and Prey: A New Ecology of Competition. *Harvard Business Review*, 71.

Osterwalder, A., Pigneur, Y., Tucci, C.L., 2005. "Clarifying business models: origins, present, and future of the concept". Communications of the Association for Information Systems 16, 1-25.

Palma F., Susi A., Tonella P., 2011. "Using an SMT Solver for Interactive Requirements Prioritization". In ESEC/FSE 2011, 48–58.

Qualypso 2013. http://www.qualipso.org. Last visited March 14th, 2013.

RRL 2013, http://earthdata.nasa.gov/esdswg/software-reuse-srwg/recommendation-documents/reuse-readiness-levels-rrls. Last visited February 15th 2013.

Soto, M.; Ciolkowski, M., 2009. "The QualOSS open source assessment model measuring the performance of open source communities". In ESEM '09, 498–501.

Teece, D.J., 2010. "Business Models, Business Strategy and Innovation". *Long Range Planning*, 43, 172–194.

Yu, E., 1995. *Modeling Strategic Relationships for Process Re-Engineering*. PhD Thesis, Department of Computer Science, University of Toronto.