CORE
Metadata, citation and similar papers at core.ac.uk
Provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

Wirtschaftsinformatik Proceedings 2015 Wirtschaftsinformatik

3-5-2015

Identification and Importance of the Technological Risks of Open Source Software in the Enterprise Adoption Context

Mario Silic

Andrea Back

Follow this and additional works at: http://aisel.aisnet.org/wi2015

Recommended Citation
Silic, Mario and Back, Andrea, "Identification and Importance of the Technological Risks of Open Source Software in the Enterprise Adoption Context" (2015). *Wirtschaftsinformatik Proceedings 2015*. 78.
http://aisel.aisnet.org/wi2015/78

This material is brought to you by the Wirtschaftsinformatik at AIS Electronic Library (AISeL). It has been accepted for inclusion in Wirtschaftsinformatik Proceedings 2015 by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Identification and Importance of the Technological Risks of Open Source Software in the Enterprise Adoption Context

Mario Silic and Andrea Back

Institut für Wirtschaftsinformatik (IWI), University of St Gallen, St. Gallen, Switzerland
{mario.silic}@student.unisg.ch
{andrea.back}@unisg.ch

Abstract. Open source software (OSS) has reshaped and remodeled various layers of the organizational ecosystem, becoming an important strategic asset for enterprises. Still, many enterprises are reluctant to adopt OSS. Knowledge about technological risks and their importance for IT executives is still under researched. We aim to identify the technological risks and their importance for OSS adoption during the risk identification phase in the enterprise context. We conducted an extensive literature review, identifying 34 risk factors from 88 papers, followed by an online survey of 115 IT executives to study the risk factors' importance. Our results will be very valuable for practitioners to use when evaluating, assessing and calculating the risks related to OSS product adoption. Also, researchers can use it as a base for future studies to expand current theoretical understanding of the OSS phenomenon related to IT risk management.

Keywords: open source software, IT risk, IT risk management, enterprise open source software, information security, OSS risk, FLOSS risk, technological risk

1 Introduction

While we could debate about open source software (OSS) still being a phenomenon or a disruptive technology, the reality is that OSS has reshaped and remodeled various layers of the organizational ecosystem, becoming an important strategic asset for enterprises. That was not always the case.

Microsoft's holy war on open source software started some years ago when the company's CEO described open source software as "a cancer that attaches itself in an

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Silic, M.; Back, A. (2015): Identification and Importance of the Technological Risks of Open Source Software in the Enterprise Adoption Context, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1163-1176

intellectual property sense to everything it touches"[1]. In 2014 Microsoft made an important announcement about its intention to move to open source its .Net platform (a very popular software framework used by software developers to build Windows applications). This decision is an important shift for the software giant and confirms the importance of the OSS movement. Indeed, not so long ago software was perceived as a product that had a certain price to be paid for it, just as we would pay for any other material object [1]. The "open source" movement started in 1998 [2] leading to the creation of the open source software (OSS). What is common to a number of different definitions of OSS that exist in academia and among practitioners is that OSS is software that can be freely modified and freely distributed, is technologically neutral, and grants free subsidiary licensing rights [2]. Today, from the enterprise perspective, OSS adoption and use have seen significant jumps; in certain areas, such as the server market, OSS technology is leading the race with over 54% [3] of all worldwide servers using OSS server products. According to the [4] survey OSS is experiencing an exponential rise in many areas such as cloud/virtualization, content management and mobile. It is evident that for many enterprises OSS has become a very legitimate option when choosing between a proprietary closed source solution and a freely available open source solution. In this context OSS is considered to be an important strategic asset thanks to its short time to market, reduced development and maintenance costs, and its customization possibilities [5]. Hence, OSS reshaped the software industry, directly impacting enterprises' business models, operating procedures and overall IT decision making chains [6-8]. However, quality and security have been important topics of dispute and debate between open and closed source opponents [9]. From an enterprise perspective 64% of enterprises still view security as a major obstacle to OSS adoption [10]. Despite this fact, many studies have not found any clear difference in security or quality levels between open and closed source software [11-15]. [16] states that open source software is not more secure than closed source software. However, [12] argues that this debate is often determined by biased attitudes where there is a lack of quantitative data to support the results. By comparing the published vulnerabilities of open and closed source software, [12] concluded that there is no significant difference in severity levels between open and closed source software. However, one limitation of the studies that compare IT security risks between open and closed source software exists in the number of cases used for comparison, which is generally very low. Another is that the majority of these studies are already outdated (produced between 2005 and 2009) and may not reflect the recent OSS expansion in terms of the new OSS products (e.g. Big data, mobile, cloud).

Still, one recent fact reveals that iOS (Apple's closed source operating system), with iPhone and iPad, is largely dominating the enterprise market with over 70% of the mobile device market share [17]. One possible explanation for this surprisingly dominant position of closed source software could be that many OSS products have a short lifecycle and end as a failure. Support for this comes from the popular OSS portal SourceForge.org, where out of more than 150,00 projects only 17% were successful

[1] http://www.cnet.com/news/dead-and-buried-microsofts-holy-war-on-open-source-software/

and over 46 percent were abandoned in the initiation stage [18]. Despite this high number of failures, OSS proponents highlight clear advantages that OSS brings for enterprises, such as lowering expenditure through reduced scaling costs, license fees, hardware needs, etc. [18, 19]. On the other hand, opponents argue that OSS adoption brings important risks and that enterprises are clearly not performing any real cost-benefit analysis [20]. In other words, the OSS evaluation process can be very time-consuming and labor-intensive and these hidden costs are just one of the potential technological risks [21]. In order to minimize these risks, it is often necessary to go through the phase of end-user training [22] and get professional support [19]. The quality of the OSS product was also questioned by researchers [19, 20, 23], along with issues of 'compatibility' and 'lack of standards' [7, 24].

Another important risk is licensing, as a number of different types of licenses exist [21, 25], which complicates the overall integration process [26]; also, the lack of documentation or a roadmap [7] could be a hindering factor when adopting OSS.

Finally, most of the previous studies face a generalizability challenge as either they were focused on a single (specific) OSS product in a particular organization/country [27] or their research setting was public administrations [28] and software companies [29]. On the other hand, the study done by [30] on the organizational adoption of OSS did not face this generalizability issue as it employed data extraction techniques to analyze the web server logs. However, in so doing it limited the scope of the OSS products it could analyze. Moreover, according to [20, 29, 31], the risks related to OSS adoption are not yet well understood, and need to be researched in a more systematic way that would bring more precision, accuracy and generalizability to the results.

In this paper we aim to fill this existing research gap by identifying the technological risks of OSS in the enterprise context. Hence, in this research paper we seek to address the following research questions:

1. What are the technological risks of OSS in the enterprise context?
2. Which technological risks of OSS have most impact on the adoption process in the enterprise context?

We will proceed as follows. Firstly, we will identify the technological risks present in the OSS enterprise adoption context by conducting an extensive literature review. Secondly, we will conduct a survey with enterprise IT decision makers to confirm the importance and relevance of the identified technological risks in their decision making process. Our research will be of particular interest to practitioners as it will offer valuable guidance during the risk identification phase. For researchers, our findings will bring new insights about the technological risks related to the OSS phenomenon. In the next sections we will 1) detail the research methodology explaining our literature review; 2) identify the OSS technological risks and review them through the sur-

vey; 3) discuss how the results can be applied in practice; and finally, 4) conclude the paper.

2 Research methodology

2.1 Identification of the technological risks in OSS - Literature review

To have the best possible literature review outcome, we followed the recommendation of conducting review stages, as suggested by [32], which consist of a four-step search process: journal search, database search, keyword search and backward/forward search.
For this literature review we adopted a broad hierarchical search strategy in order to capture high quality papers. We started with the most reliable sources and, using the backward and forward search, we added articles not identified in the previous search phase.
Following the four main steps as the core of our strategy, the initial three steps were carried out between February and June 2014, while articles in the fourth step were added on a continuous basis.

Database selection and keyword search

As the 'IT risk' topic can be found in several different disciplines, our aim was to be exhaustive in coverage. Hence, we used the following databases: EBSCOhost, ISI Web of Knowledge and Science Direct. These three databases allow for searching more than 4,000 IT/business related journals and conferences. Moreover, we included two major libraries, ACM and the IEEE Xplore, as their focus is mostly on computer science publications. Finally, we also added AIS Electronic Library as we wanted to include the Journal of the Association for Information Systems (JAIS). With this approach we covered the majority of top MIS journals. Also, in order to be as exhaustive as possible, we did not restrict the search to a defined time frame, but searched through all available years. Additionally, in order to be sure we did not omit any important publication we included Google Scholar (despite the fact that it is considered to be a rather uncontrollable source) as we wanted to ensure that all important previous work was also included.

To begin with, we followed the recommendations of [32] and [33] in conducting the review process:

1) We searched through all databases. We used the terms (("*security"* OR *"safety"* OR *"risk"* OR *"danger"* OR *"vulnerability"* OR *"attack"* OR *"threat" OR "weaknesses" OR "vulnerabilities" OR "attacks" OR "threats"*) AND ("*open source"* OR "*open source software"* OR "*open systems*")) to search through the titles, abstracts and keywords of all articles published in the respective journals in order to find all publications.

2) In order to be more comprehensive and ensure all important prior work was included, we used Google Scholar with the combination of risk / open source software / security keywords. Google Scholar offers some unique options for scientific research (e.g. [34]) and it searches articles from various disciplines and sources. The initial search of Google Scholar yielded over 2,040,000 articles. We limited the results to the first 100 articles and identified an additional 10 articles that we included in the paper stock.
3) Our last step was a backward/forward search, as suggested by [33]. While analyzing the publications identified in the previous steps, we selected articles that could be relevant (mainly publications from top journals). An additional 15 papers were identified using the backward/forward process.

Our initial paper stock comprised 145 papers. We removed 27 duplicates and, after analyzing every article for the journal and topic relevance (by reviewing the abstract), we removed an additional 30 articles. The final stock of papers comprised 88 articles.

In order to identify technological risks we proceeded as follows: 1) we extracted all already identified technology risks from our paper stock; 2) we reduced 110 initially found risk items (by merging risk items with similar meaning, and removing duplicates) to 48 risk items; and 3) we regrouped risk items. Our final number of items was reduced to 34. The regrouping of items was repeated four times. Three researchers and two independent IT consultants performed this successive refinement process. Overall, during the entire technology risks identification process we did not find any major issues (except for licensing risk factors where several similar risk items appeared) as the whole procedure relied on the previously identified risks in the OSS enterprise context.

Instrument validation

To assess objectivity, reproducibility, and inter-coder reliability in respect of our content analysis, two reliability scores were calculated to ascertain the level of agreement between coders. Firstly, we computed Krippendorff's alpha because it is generally accepted as the most relevant measure of agreement among multiple coders [35]. Secondly, Cohen's kappa [36] was calculated as it is still considered the best choice when it comes to evaluating inter-coder reliability [37]. Krippendorff's alpha and Cohen's kappa substantially exceeded the recommended minimum values of 0.70 and 0.60, respectively. Hence, we conclude that the coding instrument was deemed reliable.

2.2 Surveys

As the objective of this study is to identify the technological risks of OSS that make a difference throughout the decision making process, we launched an online survey. We asked IT decision makers to assess the technological risks by ranking them according to the importance they have during the OSS product evaluation. This importance cri-

terion relates to the risk identification phase that decision makers perform when adopting new products. To rank technological risk factors, a scale from 0-10 was used in which 0 signified "totally irrelevant" and 10 signified "absolutely fundamental". In order to minimize possible ranking challenges we clearly explained to participants that only the final ranking has a real meaning, while values have no meaning in themselves. In other words, giving the value of 7 to factor 1 and the value of 3 to factor 2 means that factor 1 is more important than factor 2, but the values of "7" and "3" have no meaning in themselves.

The survey was conducted from June to July 2014. We used e-mail to address the key informants in the following order: the Chief Information Officer (CIO) was our primary target whom we tried to contact whenever possible. However, in many cases, the CIO function did not exist and only the Chief Executive Officer (CEO) or IT directors were present. Thus, after the CIO we targeted similar functions (such as a CEO or IT director). Also, in order to make sure that we avoided any eventual data privacy or e-mail spam concerns, we did not send any reminders to the informants. Finally, in total we contacted 620 IT decision makers who represented enterprises of various sizes and types. Our aim was not specifically to target users or non-users of OSS products, as we did not want to influence the study results and create a possible bias by selecting only users of OSS technology. However, all contacted participants were involved in the IT decision making processes. This means that they were actively involved in the risk identification phase during the adoption analysis phase of the new software products. In total, 135 people completed the survey. Furthermore, we removed 20 responses due to missing data (12) and inconsistent response patterns (8) resulting from implausibly short handling times (< 3 minutes). Our final sample accounted for 115 participants.

This response rate (of 18.5%) can be seen as low but it is still acceptable with regard to the difficulties in obtaining survey responses from IS executives and corporate-level managers [38].

3 Results

In this section we present our detailed findings. Firstly, we start by presenting the technological risks present during the OSS adoption process. These technological risks are evaluated by enterprises during the risk identification phase and play an important role in the decision making process when adopting a new OSS product.

3.1 Identification of the technological risks of OSS

Using the extensive literature review followed by the risk items refinement process, the identified technological risks are presented in Table 1. A total of 34 technological risks were identified.

Table 1. Technological risk factors

Risk factors	
1. Interoperability	2. Maintainability
3. Lack of support	4. Compliance
5. Lack of ownership	6. Performance
7. Access to the source code	8. Short-term support
9. Lack of expertise	10. Environmental risks
11. Availability of technical documentation/user manual	12. Modularity
13. Mid-/long-term existence of a user community	14. Standard architecture
15. Code security	16. Law conformance
17. Ability to customize	18. Type of license
19. Portability	20. Programming language uniformity
21. Localization and human interface	22. Complexity
23. Best practices on use	24. OSS quality
25. Return on investment (ROI)	26. Evaluation
27. Total cost of ownership (TCO)	28. Code integrity
29. Sponsor	30. Compatibility issues
31. Hidden costs	32. Lack of roadmap
33. Forking	34. Reliability

3.2 Importance of the technological risks of OSS

After identifying the technological risks that have a significant effect on the IT decision making process of OSS product risk evaluation, we present the online survey results.

Participants' demographics

In Table 2 participant demographics are detailed.

Table 2. Survey participants' demographics

Country	*#*	*Country*	*#*	*Country*	*#*
Australia	3	Indonesia	1	Singapore	2
Belgium	4	Israel	2	South Africa	3
Brazil	5	Italy	5	Spain	4
Canada	4	Jordan	1	Sweden	2
Chile	2	Mexico	2	Switzerland	3
Croatia	2	Norway	2	Taiwan	1
Denmark	2	Pakistan	2	Turkey	2
Finland	2	Poland	3	Ukraine	4
France	5	Portugal	1	United Kingdom	8

Germany	3	Romania	1	United States	2
Greece	3	Russia Fed-	3	Pakistan	2
India	2				

115 IT executives completed the survey, providing responses from 34 different countries. Of these 115 participants, 102 were men (88.6%) and 13 were women (11.4%); the average age of the participants was 42.8 years.

Participants originated from various types of industries/organizations: Consulting (18.6%), Engineering (7.8%), Entrepreneurship (5.2%), Information Technology (41.2%), Banking/Finance/Accounting (1.50%), Business Services/Consultant (1.60%), and other (24.1%). In the other category there were a total of 18 different industries represented (i.e. Airport, Banking, Education, Finance, Government, etc.). When asked about their positions within these organizations, the distribution came out as follows: CIO (70.5%), IT Director (9.6%), Information Security Manager (1.5%), and other (18.40%). There were 12 different positions indicated in the other category (i.e. Architect, Business Systems Security Manager, Developer, Network Admin., etc.). When it comes to professional experience and organizational size, Table 3 shows the participant distribution.

Table 3: Participant Experience and Organization Size

Years of experience	*In %*	*Organization size*	*In %*
Less than 1 year	28 (24.3%)	Large: over 250 employees	51 (44.3%)
1–3 years	35 (30.4%)	Medium: 50–250 employees	36 (31.3%)
3–8 years	32 (27.8%)	Small: fewer than 50 employees	28 (24.4%)
Over 8 years	20 (17.5%)		

We also wanted to understand the number of "nonprofit" organizations that participated in the survey. Thus, we asked the participants whether their organization was "for profit" or "nonprofit". Only 5 participants out of 115 confirmed that their organization is a "nonprofit" one. As this is rather a low number, we decided not to compare the "for profit" vs "nonprofit" statistics as it could lead to statistically wrong results.

However, we asked participants whether they tested or evaluated OSS products before adopting them. In other words, we wanted to know if there was any formal procedure whereby an OSS product was evaluated or whether it was simply adopted without going through any risk identification phase. A high number of participants (85%) confirmed that their organization evaluates OSS products.

Finally, in Table 4 we present the detailed findings about the importance of technological risk factors which are evaluated during the risk identification phase of OSS products.

Table 4 has five different columns, the first of which indicates the risk factor. The second column indicates the overall average score the risk factor obtained, whereas the three remaining columns indicate the scores attributed by participants, divided by their enterprise size.

Table 4: Importance of the technological risk factors

		Enterprise size		
Technological risk factor	Overall	Large	Medium	Small
Security	9.6	10	9.6	9.6
Reliability	9	9.3	8.9	9
Performance	8.5	8.7	8.8	8.5
Maintainability	8.1	8.5	8.1	8.1
Lack of expertise	8.1	8.5	8.2	8.1
Access to the source code	8	6.5	7.4	8
Standard compliance	7.9	8.5	8	7.9
Availability of technical documentation/user manual	7.9	7.8	8.6	7.9
Total cost of ownership (TCO)	7.8	8.8	8	7.8
OSS quality	7.8	7	7.8	7.8
Ability to customize	7.7	7.2	7.5	7.7
Mid-/long-term existence of a user community	7.6	7.7	8	7.6
Interoperability issues	7.5	8	7.6	7.5
Return on investment (ROI)	7.5	7.8	7.9	7.5
Hidden costs	7.5	6	8.2	7.5
Law conformance	7.4	7.3	8.3	7.4
Code integrity	7.4	7.5	7.3	7.4
Mid-/long-term existence of a maintainer organization/sponsor	7.4	6.8	8.9	7.4
Standard architecture	7.3	7.2	7.5	7.3
Compatibility issues	7.3	6	8	7.3
Lack of long-term support	7.3	7.5	8	7.3
Standard architecture	7.2	7.3	7.3	7.2
Portability	7.1	6.8	6.7	7.1

Modularity	7.1	7	6.6	7.1
Best practices on use	7.1	6.4	7.6	7.1
Localization and human interface	7	7.2	7.2	7
Types of licenses used	6.9	7.5	6.7	6.9
Complexity	6.9	6.8	6.5	6.9
Short-term support	6.9	6.7	7.7	6.9
Lack of good evaluation / Testing	6.9	6.5	8	6.9
		Enterprise size		
Technological risk factor	Overall	Large	Medium	Small
OSS product complexity	6.7	5.8	6.7	6.7
Forking	6.4	5.5	6.8	6.4
Lack of ownership	6.4	7	6.6	6.4
Lack of roadmap	6.3	5	6.2	6.3
Environmental issues	5.5	6.2	5.7	5.5

4 Discussion

IT risk management is the application of risk management to information technology with the objective of better managing IT risk. This first step in the risk management process, risk identification, is a critical one as failure to achieve high security may lead to the breakdown of the whole system [39]. This study identified 34 risk factors that have significant importance for IT executives when evaluating OSS products. Our results confirm previous findings from academia [12, 16] or practitioner surveys [9, 10], confirming that security related risk ranks highest and has high importance in the entire decision making process. Comparing the top six risk factors (security, reliability, performance, maintainability, lack of expertise, and access to the source code), between different organizational sizes (large, medium and small) we can see that security risk factor is the primary concern for large enterprises and was ranked with a value of 10; we can also see that access to the source code is not an important risk factor taken into account when evaluating OSS products. This could mean that large enterprises are deeply concerned about their IT security but are not really concerned by the fact that anonymous programmers with bad intentions could modify the original source code and embed malicious code into the freely available open source code. [40]. Compliance risk, interoperability and the total cost of ownership (TCO) are factors that seem to be of high importance for large enterprises. This is not a surprising result as we were expecting to see these factors rank highly. Indeed, a study conducted by [41] analyzed 635 apps and found that more than 70% of mobile applications that contain open source fail to comply.

From an enterprise perspective, this can be seen as worrying, as expenses related to regulatory fines for compliance failure can be very high. Also, it is evident that enterprises are very cautious about interoperability and the total cost of ownership (TCO) when making their financial estimates related to the direct and indirect costs of OSS

product adoption. Among the five least important risk factors we can see that OSS product complexity, forking, lack of ownership, lack of roadmap and environmental issues do not have a high impact on the decision making process. While we could understand why the 'environmental issues' factor does not figure among the most important factors, it was a bit surprising to see that enterprises are not really worried about the OSS product complexity, lack of ownership and roadmap, or forking. Indeed, as past research has revealed that only 17% of all Sourceforge.org open source projects have been successful and over 46 percent were abandoned in the initiation stage [18], we would expect to see higher concerns from the enterprise perspective regarding the uncertainties related to the future of the project (e.g. lack of road map). This could mean that enterprises are aware of these potential pitfalls but are also comfortable with taking the risk.

Another finding is that small enterprises' results are very consistent with the overall results. This can be interpreted as the willingness of smaller companies to be more agile and open to adopting OSS products. In medium or large organizations, due to much greater organizational complexities, challenges are also higher and thus, there is a need to be much more cautious about various risk factors. One such challenge is the difference in terms of the importance of 'hidden costs' and 'compatibility issues' for large and medium-sized companies; for large companies hidden costs are not a particularly significant risk factor, while for medium-sized companies, on the contrary, this represents a risk factor that has to be carefully analyzed. The same is true of the 'compatibility issues'. This can probably be explained by the fact that larger organizations have much bigger and more complex organizational structures whereby these risk factors would usually undergo a longer and more intensive evaluation process.

Finally, our identified technological risks (Table 4) would be a very valuable tool to support the risk identification process in the context of OSS. We provide the identified list of technological risk factors that have the greatest impact on OSS adoption from the risk perspective in the enterprise context. This list could be used as a checklist that IT executives could use while evaluating the OSS product in the risk identification phase. Also, it could be an important source of valuable information for the decision makers when evaluating and quantifying the risks related to OSS organizational adoption.
Given that prior research [29, 31] has argued that technological risks related to OSS adoption are not well understood, this work attempted to bridge this research gap by providing a systematic review of the technological risks present in the enterprise context and their importance for decision makers.

Future researchers may use our results as a base from which to further explain the reasons why various risk factors have different levels of importance for enterprises. Moreover, it would be useful to further advance the theoretical understanding of the risk factors of organizational OSS.

5 Conclusion

Our research aimed at answering the following research questions: What are the technological risks of OSS adoption in the enterprise context, and which technological risks of OSS have most impact on the adoption process in the enterprise context?
We conducted an exhaustive literature review to identify the main technological risk factors from 88 papers, followed by an online survey of 115 IT executives, using the taxonomy development method suggested by [42]. Our research offers valuable insights into the technological risks present in the OSS context and the importance they have for the IT executives during the risk identification process of OSS products.

Our results could be particularly valuable for the IT executives involved in the risk management process during the risk identification phase as they could be used as a checklist when reviewing, evaluating and even calculating the risks related to OSS adoption. Future studies may further expand and build on these results to further explain the risk identification phase in the enterprise OSS context by advancing the theoretical understanding of the phenomenon.

References

1. Schryen, G.: Is open source security a myth? Communications of the ACM 54, 130-140 (2011)
2. Perens, B.: The open source definition. Open sources: voices from the open source revolution 171-185 (1999)
3. Netcraft: Web server survey. (2014) http://news.netcraft.com/archives/2013/08/09/august-2013-web-server-survey.html. (Accessed:14.07.2014)
4. Black Duck: The Eighth Annual Future of Open Source Survey. (2014) http://www.blackducksoftware.com/future-of-open-source. (Accessed:10.07.2014)
5. Franch, X., Susi, A., Annosi, M.C., Ayala, C., Glott, R., Gross, D., Kenett, R., Mancinelli, F., Ramsamy, P., Thomas, C.: Managing Risk in Open Source Software Adoption. In: Proc. 8th Int. Conf. on Software Engineering and Applications (ICSOFT-EA 2013). SciTePress. (Year)
6. Krogh, G.v.: Open-source software development. MIT Sloan Management Review 44, 14 (2003)
7. Ågerfalk, P.J., Deverell, A., Fitzgerald, B., Morgan, L.: Assessing the role of open source software in the European secondary software sector: a voice from industry. In: Proceedings of the 1st International Conference on Open Source Systems (Scotto, M. and Succi, G. Eds.), pp. 82-87. (Year)
8. Ågerfalk, P.J., Fitzgerald, B.: Outsourcing to an Unknown Workforce: Exploring Opensurcing as a Global Sourcing Strategy. MIS quarterly 385-409 (2008)
9. Gartner: Road Map for Open-Source Success Understanding Quality and Security. (2014) http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=2674615&ref=QuickSearch&sthkw=Road+Map+for+Open-Source+Success%3A+Understanding+Quality+and+Security. (Accessed:14.07.2014)

10. Deloitte: Open mobile survey. (2012) http://www.deloitte.com/assets/Dcom-Turkey/Local%20Assets/Documents/turkey_tr_tmt_openmobile_220212.pdf. (Accessed:10.07.2014)
11. Dedeke, A.: Is Linux Better than Windows Software? IEEE Software 26, 104-104 (2009)
12. Schryen: Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. AMCIS 2009 Proceedings (2009)
13. Schryen, G., Rich, E.: Increasing Software Security through Open Source or Closed Source Development? Empirics Suggest that We have Asked the Wrong Question. In: System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pp. 1-10. (Year)
14. Schryen: Is Open Source Security a Myth? Communications of the ACM 54, 130-140 (2011)
15. Aberdour, M.: Achieving Quality in Open-Source Software. Software, IEEE 24, 58-64 (2007)
16. Payne, C.: On the security of open source software. Information Systems Journal 12, 61-78 (2002)
17. Good Technology: Report on App, Platform and Device Preferences from the Leader in Secure Mobility. (2013) http://media.www1.good.com/documents/rpt-mobility-index-q413.pdf. (Accessed:10.07.2014)
18. Schweik, C.M., English, R.C.: Internet success: a study of open-source software commons. MIT Press (2012)
19. Fitzgerald, B., Kenny, T.: Developing an information systems infrastructure with open source software. Software, IEEE 21, 50-55 (2004)
20. Ven, K., Verelst, J., Mannaert, H.: Should you adopt open source software? Software, IEEE 25, 54-59 (2008)
21. Tiangco, F., Stockwell, A., Sapsford, J., Rainer, A., Swanton, E.: Open-source software in an occupational health application: the case of Heales Medical Ltd. Procs (2005)
22. Morgan, L., Finnegan, P.: Benefits and drawbacks of open source software: an exploratory study of secondary software firms. Open Source Development, Adoption and Innovation, pp. 307-312. Springer (2007)
23. Rudzki, J., Kiviluoma, K., Poikonen, T., Hammouda, I.: Evaluating Quality of Open Source Components for Reuse-Intensive Commercial Solutions. In: Software Engineering and Advanced Applications, 2009. SEAA '09. 35th Euromicro Conference on, pp. 11-19. (Year)
24. van Rooij, S.W.: Perceptions of Open Source versus Commercial Software: Is Higher Education Still on the Fence? Journal of Research on Technology in Education 39, 433-453 (2007)
25. McGhee, D.D.: Free and open source software licenses: benefits, risks, and steps toward ensuring compliance. Intellectual Property & Technology Law Journal 19, 5 (2007)
26. Jaaksi, A.: Experiences on product development with open source software. Open source development, adoption and innovation, pp. 85-96. Springer (2007)
27. Goode, S.: Something for nothing: management rejection of open source software in Australia's top firms. Information & Management 42, 669-681 (2005)
28. Federspiel, S.B., Brincker, B.: Software as Risk: Introduction of Open Standards in the Danish Public Sector. Information Society 26, 38-47 (2010)

29. Hauge, Ø., Ayala, C., Conradi, R.: Adoption of open source software in software-intensive organizations–A systematic literature review. Information and Software Technology 52, 1133-1154 (2010)
30. Spinellis, D., Giannikas, V.: Organizational adoption of open source software. Journal of Systems and Software 85, 666-682 (2012)
31. Nagy, D., Yassin, A.M., Bhattacherjee, A.: Organizational adoption of open source software: barriers and remedies. Communications of the ACM 53, 148-151 (2010)
32. Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the giant: On the importance of rigour in documenting the literature search process. In: ECIS, pp. 2206-2217. (Year)
33. Webster, J., Watson, R.T.: Analyzing the past to prepare. MIS quarterly 26, 13-23 (2002)
34. Henderson, J.: Google Scholar: A source for clinicians? Canadian Medical Association Journal 172, 1549-1550 (2005)
35. Hayes, A.F., Krippendorff, K.: Answering the call for a standard reliability measure for coding data. Communication methods and measures 1, 77-89 (2007)
36. Cohen, J.: Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit. Psychological bulletin 70, 213 (1968)
37. Dewey, M.E.: Coefficients of agreement. The British Journal of Psychiatry 143, 487-489 (1983)
38. Poppo, L., Zenger, T.: Do formal contracts and relational governance function as substitutes or complements? Strategic management journal 23, 707-725 (2002)
39. Slovic, P.E.: The perception of risk. Earthscan Publications (2000)
40. Sans: Security Concerns in Using Open Source Software for Enterprise Requirements. (2009) http://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305. (Accessed:02.07.2014)
41. OpenLogic: OpenLogic Scan. (2011) http://www.openlogic.com/news/bid/154650/OpenLogic-Scan-Shows-Open-Source-License-Violations-for-iPhone-and-Android-More-Than-70-Of-Mobile-Applications-Containing-Open-Source-Fail-to-Comply. (Accessed:02.07.2014)
42. Nickerson, R.C., Varshney, U., Muntermann, J.: A method for taxonomy development and its application in information systems. European Journal of Information Systems 22, 336-359 (2013)