Preliminary Results from a State-of-the-Practice Survey on Risk Management in Off-The-Shelf Component-Based Development

Jingyue Li[1], Reidar Conradi[1,2], Odd Petter N. Slyngstad[1], Marco Torchiano[3], Maurizio Morisio[3], and Christian Bunse[4]

[1]Department of Computer and Information Science,
Norwegian University of Science and Technology (NTNU),
NO-7491 Trondheim, Norway
{jingyue, conradi, oslyngst}@idi.ntnu.no
[2]Simula Research Laboratory, P.O.BOX 134, NO-1325 Lysaker, Norway
[3]Dip.Automatica e Informatica, Politecnico di Torino
Corso Duca degli Abruzzi, 24, I-10129 Torino, Italy
{morisio, marco.torchiano}@polito.it
[4]Fraunhofer IESE, Sauerwiesen 6,
D- 67661 Kaiserslautern, Germany
Christian.Bunse@iese.fraunhofer.de

Abstract. Software components, both Commercial-Off-The-Shelf and Open Source, are being increasingly used in software development. Previous studies have identified typical risks and related risk management strategies for what we will call OTS-based (Off-the-Shelf) development. However, there are few effective and well-proven guidelines to help project managers to identify and manage these risks. We are performing an international state-of-the-practice survey in three countries - Norway, Italy, and Germany - to investigate the relative frequency of typical risks, and the effect of the corresponding risk management methods. Preliminary results show that risks concerning changing requirements and effort estimation are the most frequent risks. Risks concerning traditional quality attributes such as reliability and security of OTS component seem less frequent. Incremental testing and strict quality evaluation have been used to manage the possible negative impact of poor component quality. Realistic effort estimation on OTS quality evaluation helped to mitigate the possible effort estimation biases in OTS component selection and integration.

1 Introduction

OTS components (Off-The-Shelf) includes COTS (Commercial-Off-The-Shelf) and OSS (Open Source Software) components. More and more software projects start to use OTS components. However, using such external components introduces many risks [1, 3, 4, 5]. Before project managers decide to acquire an external component, instead of building it in-house, they must identify possible risks. Although several

risks and risk management strategies in OTS-based development have been identified [1-7, 10, 11, 14] from case studies, few empirical studies have been done to verify their conclusions. As a result, software project managers have few effective and well-proven guidelines to identify the relative effects of the various risks, and to manage them properly.

We designed a questionnaire to perform a state-of-the-practice study on risk management in OTS component-based development. The survey is being performed in three European countries (Norway, Italy, and Germany). We currently have gathered 42 filled-in questionnaires.

The findings of this study show that some risks are more frequent than others, such as the ability of OTS components to follow requirement changes, and estimating effort in component selection and integration. Results also show that some risk management methods, such as serious consideration of quality of the component in the selection process, helped to mitigate effort estimation risks in the selection and integration phase.

The rest of this paper is organized as follows: Section 2 introduces some related work. Section 3 describes our research design. Section 4 presents the preliminary results, and Section 5 discusses them. Conclusions and future work are presented in section 6.

2 Background

Risks are factors that may adversely affect a project, unless project managers take appropriate countermeasures. Risk management in software development has been studied for many years [8, 9, 15, 18]. These studies have proposed classical risks and risk management in software development. In addition to the classical risks associated with developing large systems, OTS components requires managers to modify their typical mitigation strategies for some of the classic risks and to develop new mitigation strategies for risks that are particular to the use of OTS component in a system.

2.1 Risks in OTS component-based development

Different stakeholders, such as component providers, component integrators, and customers, may face different kinds of risks [12]. Risks relevant to the component integrators in OTS components-based development [1, 3, 12, 11, 13, 14] are a subset of risks in component-based development, COTS-based and Open Source based development. Typical risks in OTS components-based cover different phases of a project as showed in Table 1.

Table 1. Typical risks in OTS-component based development.

Phase	ID	Possible risks
Project plan phase	R1	The project was delivered long after schedule [1].
	R2	Effort to select OTS components was not satisfactorily

		estimated [3].
	R3	Effort to integrate OTS components was not satisfactorily estimated [1].
Requirement phase	R4	Requirement were changed a lot [3].
	R5	OTS components could not be sufficiently adapted to changing requirements [3].
	R6	It is not possible to (re) negotiate requirements with the customer, if OTS components could not satisfy all requirements [14].
Component integration phase	R7	OTS components negatively affected system reliability [12,13].
	R8	OTS components negatively affected system security [11, 12, 13]
	R9	OTS components negatively affected system performance [11,12, 13]
	R10	OTS components were not satisfactorily compatible with the production environment when the system was deployed [12]
System maintenance and evolution	R11	It was difficult to identify whether defects were inside or outside the OTS components [3].
	R12	It was difficult to plan system maintenance, e.g. because different OTS components had asynchronous release cycles [1].
	R13	It was difficult to update the system with the last OTS component version [1].
Provider relationship management	R14	Provider did not provide enough technical support/ training [1, 10].
	R15	Information on the reputation and technical support ability of provider were inadequate [1, 10].

2.2 Risk management in OTS component-based development

To manage possible risks in OTS component-based development, some previous studies have proposed risk management strategies based on case studies and lessons learned [1, 3, 14, 18]. The most typical ones are summarized in Table 2.

Table 2. Typical risk management strategies in OTS-component based development.

ID	Risk management strategies
M1	Customer had been actively involved in the “acquire” vs. “build” decision of OTS components [7, 14].
M2	Customer had been actively involved in OTS component selection [7].
M3	OTS components were selected mainly based on architecture and standards compliance, instead of expected functionality [18]
M4	OTS components qualities (reliability, security etc.) were seriously con-

	sidered in the selection process [3, 14]
M5	Effort in learning OTS component was seriously considered in effort estimation [3]
M6	Effort in black-box testing of OTS components was seriously considered in effort estimation [3, 14]
M7	Unfamiliar OTS components were integrated first [1]
M8	Did integration testing incrementally (after each OTS component was integrated [14]
M9	Local OTS-experts actively followed updates of OTS components and possible consequences [14].
M10	Maintained a continual watch on the market and looked for possible substitute components [14].
M11	Maintained a continual watch on provider support ability and reputation [1].

3 Research design

3.1 Research questions

Our study was designed to address two basic research questions:

- **RQ1**: *What are the risks that software project managers met most frequently in OTS component-base development?*
- **RQ2**: *Can performed risk mitigation actions help to mitigate the corresponding risks?*

3.2 Research method

3.3 Questionnaire design

The questionnaire includes three main sections:

- Background questions to collect information of the company, project, and respondents.
- Main questions about risk and risk management. The risks and risk management strategies selected in the questionnaire are the most typical ones as showed in Table 1 and Table 2. Respondents are asked to give their opinions on these risks and risk management actions as “don’t agree at all”, “hardly agree”, “agree somewhat”, “agree mostly”, “strongly agree”, or “don’t know”. We assign an ordinal number from 1 to 5 to the above alternatives (5 meaning strongly agree).

- Questions to collect information about OTS components actually used in their project.

3.4 Concepts used in this study

Concepts used in the questionnaire are listed in the start of the questionnaire.

Component: Software components are program units of independent production, acquisition, and deployment and which can be composed into a functioning system. We limit ourselves to components that have been explicitly decided either to be built from scratch or to be acquired externally as an OTS-component. That is, to components that are not shipped with the operating system, not provided by the development environment, and not included in any pre-existing platform.

An OTS component is a component provided (by a so-called provider) from a commercial vendor or the Open Source community. An OTS component may come with certain obligations, e.g. payment or licensing terms. An OTS component is not controllable, in terms of provided features and their evolution. An OTS component is mainly used as closed source, i.e. no source code is usually modified, and even it may be available.

3.5 Data collection

3.5.1 Sample definition

The unit of this study is a completed software development project, and its OTS-relevant properties. The projects were selected based on two criteria:

- The project should use one or more OTS components
- The project should be a finished project, possibly with maintenance, and possibly with several releases.

3.5.2 Sample selection and data collection

We used random selection to gather a representative sample.

- In Norway, we gathered a company list from the Norwegian "Census Bureau" (SSB) [17]. We included mostly companies which were registered as IT companies. Based on the number of employees, we selected the 115 largest IT companies (100 IT companies and 15 IT departments in the largest 3 companies in 5 other sectors), 150 medium-sized software companies (20-99 employees), and 100 small-sized companies (5-19 employees) as the original contacting list.
- In Italy, we first got 43580 software companies from "yellow pages". We then randomly selected companies from them. For these randomly selected companies, we read their web-site to ensure they are software companies or not. 196 companies were finally clarified as software companies, and were used as the original contacting list.

- In Germany, we selected name list from a company list from an organization similar to the Norwegian "*Census Bureau*". We then used the existing IESE customer database to get contact information.

In the end, we aim for more than 150 filled-in questionnaires to have statistically valid results.

The final questionnaire was first designed and pre-tested in English (internal and external previews). It was then translated into the native languages and published on the SESE web survey tool [19] at Simula Research Lab in OSLO. Possible respondents were contacted first by telephone. If they have suitable OTS-based projects and would like to join our study, a username and password was sent to them, so that they could use the SESE web tool to fill in the questionnaire (they could also use a paper version or electronic word version). The respondents who didn't want to answer the questionnaire were also registered. We logged the main reasons of non-response, such as no software development, no OTS-based projects, and busy.

4 Results

Although the data collection process is still on-going, we have already gathered results from 42 projects (33 from Norway, 9 from Italy).

4.1 Companies and projects

The filled-in questionnaires come from 18 small, 11 medium-sized and 8 large companies. 19 are software vendors, 15 are IT consulting companies one is in Telecom, and two are IT branches of the traditional industry.

We selected one project in 35 companies. We also selected more than one different project from two large companies. Most projects used more than 10 person-months in the development phases. The developed software systems also cover different application domains as showed in Table 3.

Table 3. The distribution of the application domains of the systems

Application domains	Percentage
Bank/Finance/Insurance	19%
Other private services (consulting, wholesale, retail, etc.)	19%
Public sector	29%
ICT sector	16%
Traditional industry/engineering/construction	17%

4.2 Respondents

Most respondents have a solid IT background. Four respondents are IT managers, 17 are project managers, 18 are software architects, and three are senior software developers. 90% of them have more than three years of software development experience, and 86% of them have more than two years working experience with OTS-based development.

4.3 Answers to research questions

4.3.1 Frequency of risk occurrence

For the relative importance of the risks we listed 15 in the questionnaire, the distribution of their relative frequencies are showed in the following Fig 1.

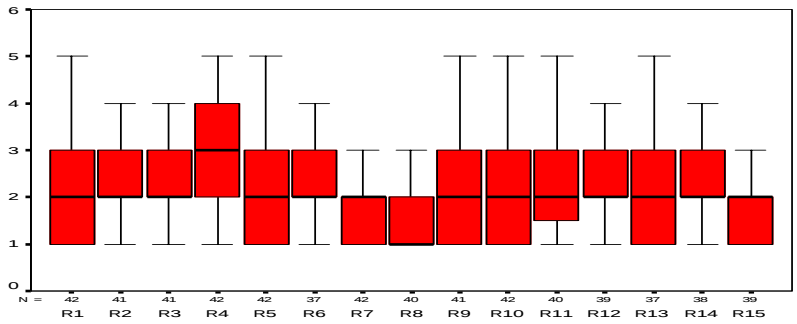

Fig. 1. Frequency of the risk occurrence

Based on distribution of these risks, we can classify the relative frequency of these risks into four categories from the most frequent to the least frequent:

- Risk R4 is the most frequent risk.
- Risks R2, R3, R6, R12, and R14 are classified as the second most frequent risks because they have an up-skewed distribution.
- Risk R1, R5, R9, R10, R11 and R13 are the third most frequent risks.
- Risk R7, R8, and R15 are the least frequent risks. These risks have either a lower median or a down-skewed distribution.

The results show that some risks were more frequent than others, such as requirement relevant risks (R4 and R6), cost-estimation risks (R2 and R3), maintenance plan risk (R12), and provider support risks (R14). Some risks relevant to OTS components reliability (R7) and security (R8) were less frequent.

4.3.2 Frequency of risks management actions

For the risk management actions, their relative frequencies are showed in Fig. 2.

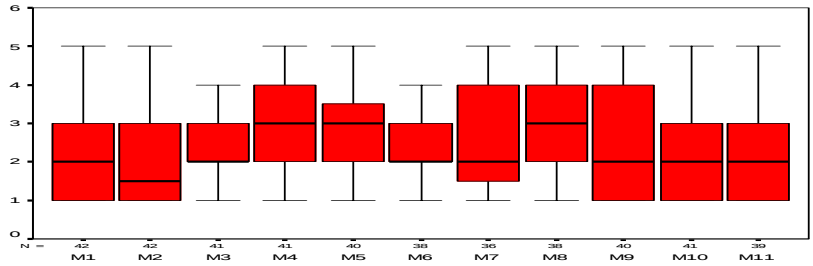

Fig. 2. Frequency of the performed risk management actions

Based on distribution of these performed risk management actions, we can classify them into three categories from the most frequent to the least frequent:

- Risk management action M4, M5, and M8 are the most frequently used methods.
- Risk management action M3 and M6 are the second most frequent methods.
- Other risk management actions as M1, M2, M7, M9, M10, and M11 are the least frequent.

The results show that quality control methods, such as quality evaluation in selection (M4) and incremental testing (M8) were used much in practice. Results also show that possible effort in learning OTS components was seriously considered (M5). However, risk management methods relevant to customers (M1, M2) and providers (M9, M10, and M11) were seldom used.

4.3.3 Relationships between risks and risk management actions

Although many risk management actions were proposed to mitigate possible risks, we investigated only the most frequent ones, i.e. M4, M5, and M8. The reason is that it is not reliable to verify the effect of risk management methods if they have rarely been used.

We calculated the correlation between risk mitigation actions performed and their corresponding risks using *Somers's d* analysis method (in SPSS version 11.0). We regarded the frequency of risks as a dependent variable and risk management actions as an independent variable. A negative correlation between them means that the more the risk management action performed, the less frequent is the risk. Only M4 showed significant effect on corresponding risks as in Table 4.

Table 4. Correlation between M4 and corresponding risks.

Risks	Risk management actions	Correlation	P-value
R2	M4	-.307	.018
R3	M4	-.327	.013

The results show that if an integrator has taken seriously consideration on the quality of the OTS component, they will plan the effort on OTS selection more completely. In addition, the effort on OTS component integration can easily be estimated. This is possibly because the actual OTS component did not cause much quality problems in the whole system after its integration.

5 Discussions

5.1 Comparison with related work

In OTS component-based development, many typical risks and risk management methods have been proposed. Our study contributed to show their relative frequency in practice. Our study also studied the effect of some risk mitigation actions to corresponding risks.

- Our findings show that the **requirement** relevant risks are the most frequent risks. The customer requirements were changed a lot. It was difficult for OTS components to follow these changes, and it is difficult to (re) negotiate the requirements because of OTS components' inability to satisfy all requirements.
- Our findings also show that **estimation of selection and integration costs** in OTS-based projects is perceived as a challenge. These results make sense intuitively, as saving time and effort is the main perceived advantage of using OTS components [4]. Most proposed risk mitigation methods focus on solving this problem by having experienced project manager or a formal cost-estimation model [2]. Our results show that giving complete estimation on the possible effort in OTS component quality evaluation helped to mitigate these risks.
- Most previous studies regard OTS components' negative effect on the **reliability and security** of the system is very challenging in OTS-based development [1, 4, 5, 6, 7, 10]. Our results show that they are not as frequent as assumed. The possible reason is that project managers used careful selection and incremental testing to help to mitigate OTS components' negative impact on the quality of the system.

5.2 Threats to validity

5.2.1 Construct validity

In this study, most risks and risk management strategies variables are taken directly, or with little modification, from existing literature. The questionnaire was pre-tested using a paper version by 10 internal experts and 8 industrial respondents. About 15% questions have been revised based on pre-test results.

5.2.2 Internal validity

We proposed to offer respondents participated in this study a final report and a seminar to share experience. The respondents were persons who want to share their experience and want to learn from others. In general, we think that the respondents have answered truthfully.

5.2.3 Conclusion validity

This study is still on-going. A larger sample will be gathered to give more significant statistical support on conclusion of this study.

5.2.4 External validity

We used different random selection strategies to select samples in different countries. It is because the limited availability of the necessary information. In Italy, there is no official organization as a national "Census Bureau" in Norway and Germany. The samples have to be selected from "yellow pages". The methods problems by performing such a survey in three countries will be elaborated in a future paper. Another possible limitation is that our study focused on fine-grained OTS components. Conclusions may be different in projects using complex and large OTS product, such as ERP, Content management system.

6 Conclusions and future work

More and more IT companies start to use OTS components in their software development projects. In addition to the classical risks for developing large systems, using OTS components brings additional risks. It therefore requires new mitigation strategies to manage these risks. In this study, we investigated the frequency of risks and risk management actions in 42 finished OTS component-based projects. The contribution of this study can be summarized into three categories:

- Risks relevant to **requirement changes and cost-estimation** happened more frequent than reliability and security risks regarding OTS components.
- Some risk mitigation methods, such as **incremental testing and strict OTS component quality evaluation** have been used more frequent than others.
- If the integrator **seriously considered the possible effort on the quality evaluation** of OTS components, it helped to solve the effort estimation risks in the OTS selection and integration.

The data collection is still on-going. More data will be gathered to give further support to conclusions in this paper. Based on the results of this survey, we will do more qualitative studies to investigate the underlying cause-effect of risk management strategies. Some typical projects in this survey will be selected as targets for the next steps.

7 Acknowledgements

This study was partially funded by the INCO (INcremental COmponent based development) project [15]. We thank the colleagues in these projects, and all the participants in the survey

8 References

1. Louis C. Rose: Risk Management of COTS based System development. Component-Based Software Quality - Methods and Techniques, LNCS Vol. 2693, Springer (2003) 352-373.
2. Chris Abts, Barry W. Boehm, and Elisabeth B. Clark: COCOTS: A COTS Software Integration Lifecycle Cost Model - Model Overview and Preliminary Data Collection Findings. Technical report USC-CSE-2000-501, USC Center for Software Engineering, 8 March 2000, Available at: http://sunset.usc.edu/publications/TECHRPTS/2000/usccse2000-501/usccse2000-501.pdf.
3. Barry W. Boehm, Dan Port, Ye Yang, and Jesal Bhuta: Not All CBS Are Created Equally COTS-intensive Project Types. Proceedings of the 2nd International Conference on COTS-Based Software Systems (ICCBSS'03), Ottawa, Canada, February (2003), LNCS Vol. 2580, Springer (2003) 36-50.
4. J. Voas: COTS Software – the Economical Choice?. IEEE Software, March/April (1998), 15(2):16-19.
5. J. Voas: The challenges of Using COTS Software in Component-Based Development. IEEE Computer, June (1998), 31(6):44-45.
6. Gerald Kotonya and Awais Rashid: A Strategy for Managing Risk in Component-based Software Development. Proceedings of the 27th EUROMICRO Conference 2001, Warsaw, Poland, September (2001) 12-21.
7. COTS risk factor. Available at: http://www.faa.gov/aua/resources/cots/Guide/CRMG.htm
8. Tony Moynihan: How Experienced Project Managers Assess Risk. IEEE Software, May/June (1997), 14 (3): 35-41.
9. Janne Ropponen and Kalle Lyytinen: Components of Software Development Risk: How to Address Them? A Project Manager Survey. IEEE Transactions on Software Engineering, February (2000), 26(2): 98-112.
10. Brian Fitzgerald: A Critical Look at Open Source. IEEE Computer July (2004), 37 (7): 92-94.
11. G. Lawton: Open Source Security: Opportunity or Oxymoron? IEEE Computer, March (2002), 35(3): 18-21.
12. Padmal Vitharana: Risks and Challenges of Component-Based Software Development. Communications of the ACM, August (2003), 46(8): 67-72.
13. Michel Ruffin and Christof Ebert: Using Open Source Software in Product Development: A Primer. IEEE Software January/February (2004), 21(1): 82-86.
14. Jingyue Li, Finn Olav Bjørnson, Reidar Conradi, and Vigdis By Kampenes: An Empirical Study of Variations in COTS-based Software Development Processes in Norwegian IT Industry. Proceedings of the 10th IEEE International Metrics Symposium (Metrics'04), Chicago, USA, September 14-16 (2004) 72-83.
15. INCO project description, 2000, http://www.ifi.uio.no/~isu/INCO
16. Thomas A. Longstaff, Clyde Chittister, Rich Pethia, Yacov Y. Haimes: Are we forgetting the risks of information technology? IEEE Computer, December (2000), 33(12): 43-51.
17. Norwegian Census Bureau: http://www.ssb.no
18. M. Torchiano and M. Morisio, "Overlooked Facts on COTS-based Development", IEEE Software, March/April 2004, 21(2): 88-93.
19. Simula SESE tool: http://sese.simula.no