ENHANCEMENT OF VECTOR METHOD BY ADAPTING OCTAVE FOR RISK ANALYSIS IN LEGACY SYSTEM MIGRATION

AIDA HAKEMI

A project report submitted in fulfillment of the requirements
for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

This project is dedicated to my family for their endless support and encouragement

ACKNOWLEDGEMENT

First and foremost, I would like to express my utmost gratitude to my supervisor, Dr..Imran Ghani for being a dedicated mentor as well as for his valuable and constructive suggestions that enabled this project to run smoothly.

Last but not least, I am forever indebted to all my family members for their constant support throughout the entire duration of this project. Their words of encouragement never failed to keep me going even through the hardest time and it is here that I express my sincerest gratitude to them.

ABSTRACT

Risk is involved in all phases of the software life cycle, and due to these risks, software can face various problems that can cause the different negative outcomes and sometimes in extreme cases failure of the software. Most of these risks lie in the migration of legacy software process. These risks can cause to create many problems, and in the worst case they can cause to failure of migration project. This project explores different types of risk analysis methods like CRAMM, CORAS, OCTAVE and VECTOR. After comparing of all these methods the author choose two suitable of these methods (OCTAVE and VECTOR). With using these two methods the project also suggests the enhanced EOV method for risk analysis in migration of legacy software.

ABSTRAK

Risiko yang terlibat dalam semua fasa kitaran hayat perisian, dan disebabkan oleh risiko-risiko ini, perisian boleh menghadapi pelbagai masalah yang boleh menyebabkan kesan negatif yang berbeza dan selalunya dalam kes kegagalan perisian. Kebanyakan risiko terletak dalam penghijrahan proses perisian legasi. Risiko-risiko ini boleh menyebabkan untuk mewujudkan banyak masalah, dan dalam hal yang paling teruk ia boleh menyebabkan kegagalan projek migrasi. Projek ini meninjau jenis kaedah analisis risiko seperti CRAMM, CORAS, oktaf dan VECTOR. Selepas membandingkan semua kaedah ini penulis memilih dua sesuai kaedah ini (OCTAVE dan VECTOR). Dengan menggunakan kedua-dua kaedah projek ini juga menunjukkan kaedah EOV dipertingkatkan untuk analisis risiko dalam penghijrahan perisian legasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Development in computer and software technology, have made this technology part of everyone's daily life. Despite of advance in software technology and created demands for various applications, existing legacy applications that have different kind of problems for organization do not have justification for used them. Therefore these systems should be migrated to new one, which can work to new environment. In migrate process there are existing risks that maybe create problem for process, so before start migration process possible risks should be analyzed.

A simple existing definition of risk is "a problem that has not yet happened but which could cause some loss or threaten the success of the project if it did". In this project risk analysis has a serious role before spreading a new application technology. For finding the possible risks of a new technology deployment project, someone should know how a suitable basic risk analysis can be performed.

Numbers of methods have been proposed for risk analysis such as OCTAVE, VECTOR MATRIX, CRAMM and etc.

1.2 Statement of the Problem

One of the most important and difficult activity of the software engineering is security maintenance in migration of legacy system to a new system.

Security maintenance is considerable because two-thirds of a software system's lifetime cost involves maintenance. Figure 1.1 shows the percentage of costs in each phase of software life cycle. (Kagan Erdil, 2003)

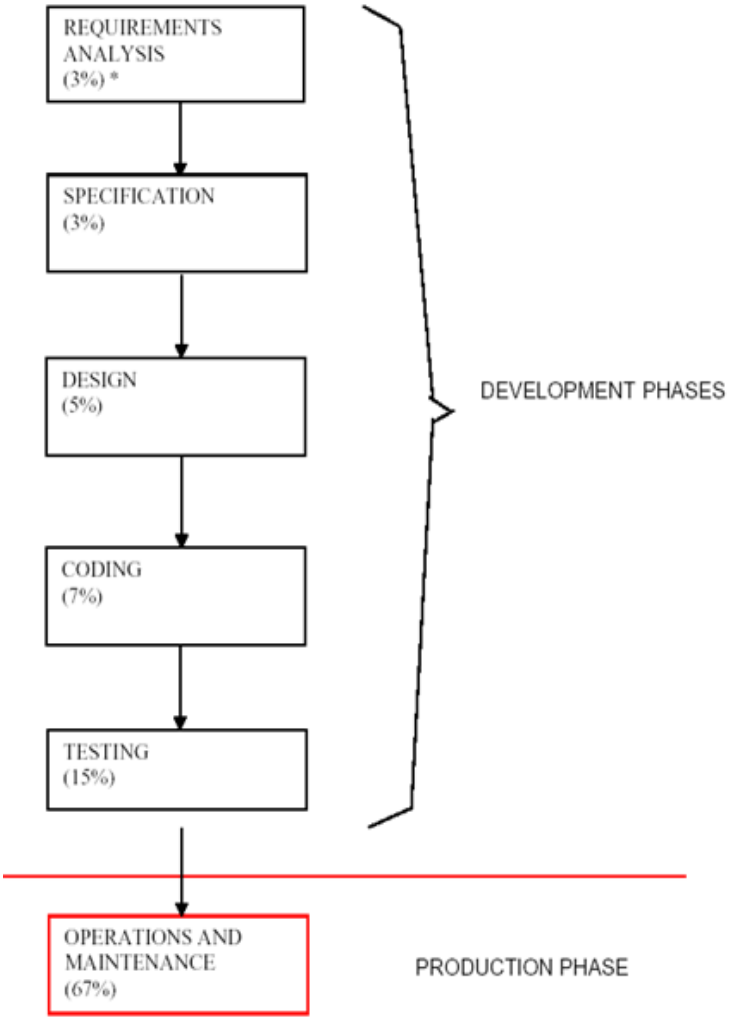

Figure 1.1: The percentage of costs in each phase of software life cycle.

Risk may appear in every kind of investment. If a company wants to change legacy software to a new one, it has to count the risk of failure and other possible

hazards. To decrease the risks and attempt in this phase using a suitable risk analysis is necessary. The aim of any risk analysis is providing decision-makers with the best possible information about the probability of loss. As a result, it is important that decision-makers accept the risk analysis method used, and that information resulting from the analysis has to in a useful form.

Given the importance of object, there are a few researches about risk analysis of this part until now. So this project is tried to search and study of risk analysis methods and finds suitable methods for analysis possible risks in migration of legacy software. These methods should be used in a combination together to achieve better results of risk assessment.

1.3 Purpose of Study

By the development of computer technology, the backbone of software was introduced widely. The same as other technology, however, software has many benefit in the world, but it has many problems too, which may accrue after release of software. One of these problems is: legacy software that was developed in the past and now it is critical to the business in which the system operates. There are two problems which often dependent to legacy system, difficult to understand and expensive to maintain. Today many legacy software Becomes to dilemma. These systems are actually critical, but maintaining them incurs unjustifiable expense.

Maintenance engineer should migrate legacy software to new one. But before this, risk analyst should analysis risks that may accrue in migrate project. The purpose of this project is suggesting hybrid method for analysis risks that may accrue during the migration process. (Improve the risk analysis of migration process, for security maintenance).

1.4 Objectives of Study

- To study and compare existing information security risk analysis methods and choose suitable methods for migration of software.
- To propose enhanced risk analysis method for migration process.
- To implementation and evaluate the enhanced method.

1.5 Scope of the Study

In order to reach the objectives stated above, the scope of this study is limited to the following:

- This study takes into information security risk analysis methods.
- This study focuses on risk analysis in migration process.
- Project evaluation is accomplished by Distribute risk analysis questionnaire for evaluate risk analysis for reason that legacy software wants to migrate to new software.

1.6 Research Questions

The questions in this report which are going to be discussed can be mentioned as follow:

- What are the current phases in migration of software?
- What are the current risk analysis methods?
- What are the suitable methods which can analyze existing risks for migration process?
- How to improve risk analysis in migration process?

1.7 Significance of the Study

This research increase software engineering's ability for developing software and tries for keep the software up to date with environment changes. Risk analysis in migration process can show the risks and importance of them and also provide enough information to deal with the risk. Also in migration legacy software, risk analysis can find risks, evaluate of them and provide information to deal with the risk.

1.8 Organization of Report

The project is organized in the following way, chapter 1 explains the problem background, problem statement, project aims, project objectives, project scopes and significant of the project. Chapter 2 presents literature review. Chapter 3 discusses on the project methodology. Followed by, chapter 4 presents the explanation in detail of proposed design of algorithm. Similarity chapter 5 composes of algorithm testing and evaluation. Finally chapter 6 is comprised of discussion and future work.

REFERENCES

Bing Wu, D. L., Jesus Bisbal, D O'Sullivan, Ray Richardson. (1997). Legacy Systems Migration - A Method and its Tool-kit Framework.

Breier, J., & Hudec, L. (2011). *Risk analysis supported by information security metrics*. Paper presented at the Proceedings of the 12th International Conference on Computer Systems and Technologies, Vienna, Austria.

Choudhari, J., & Suman, U. (2012). Story Points Based Effort Estimation Model for Software Maintenance. *Procedia Technology*, *4*, 761-765.

Christopher Alberts, A. D., James Stevens, Carol Woody. (August 2003). Introduction to the OCTAVE® Approach.

Comparing Migration Methodologies. (2007).

Cummings, C. Choosing the Best Risk Assessment Model.

Davor Maček, I. M., Nikola Ivković. (2011). Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods.

Junaid Ahsenali Chaudhry, M. A. B., Ms. Rafhana Abd Rashid. (2012). Information Security Risk Analysis Methods.

Er, M. C. (1984). Problems and solutions in software maintenance. *Data Processing, 26*(6), 25-27. doi: http://dx.doi.org/10.1016/0011-684X(84)90275-2

Jesus Bisbal, D. L., Ray Richardson, Donie O'Sullivan,. A Survey of Research into Legacy System Migration.

K.K Aggarwal, Y. S. (2007). software requirements analysis and specification.

Kagan Erdil, E. F., Kevin Keating. (2003). Software Maintenance

Ketil Stølen, F. d. B., Theo Dimitrakos, Rune Fredriksen. Model-based risk assessment – the CORAS approach.

Mahmoodian, N., Abdullah, R., & Murad, M. A. A. (2010, 15-17 June 2010). *Text-based classification incoming maintenance requests to maintenance type.* Paper presented at the Information Technology (ITSim), 2010 International Symposium in.

Martin Butler, B. W. (2010). Reducing Costs and Improving Agility Through Legacy Migration.

Muhammad Inayat Ullah, M. S., Nazir Muhammad. (2010). reduction of enhanced maintenance effort using ARM model and RMMM plan.

Patterson, F. D., & Neailey, K. (2002). A Risk Register Database System to aid the management of project risk. *International Journal of Project Management, 20*(5), 365-374. doi: http://dx.doi.org/10.1016/S0263-7863(01)00040-0

Pyka Marek, J. P. (2006). The OCTAVE methodology as a risk analysis tool for business resources.

Talabis, M., & Martin, J. (2013). Chapter 2 - Information Security Risk Assessment: A Practical Approach *Information Security Risk Assessments* (pp. 27-62). Boston: Syngress.

Tsiakis, T. (2010). Information Security Expenditures: a Techno-Economic Analysis. *International Journal of Computer Science and Network Security (IJCSNS), 10*(4), 7-11.

Vorster, A., & Labuschagne, L. (2005). *A framework for comparing different information security risk analysis methodologies*. Paper presented at the Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, White River, South Africa.

Williams, L. (2007). Security Risk Analysis.

Yazar, Z. (2002). A Qualitative Risk Analysis and Management Tool - CRAMM.