Proclaim! (or Read!) In The name of thy Lord and cherisher, who created, Created man, out of a (mere) clot of congealed blood: Proclaim! and Thy Lord is most Bountiful, He who Taught (the use of) the Pen, Taught man that which he knew not. Nay, but man doth transgress all bounds, In that he looketh upon himself as self-sufficient.
SoftRisk: Prototype for Software Risk Management

A thesis Submitted to the
Faculty of Computer Science and Information Technology
University of Malaya

In fulfillment of the requirements for the degree of
Master of Computer Science

By
Ayad Ali Keshlaf
March 1999

Faculty of Computer Science and Information Technology
University of Malaya
Malaysia
PUBLICATIONS FROM THE RESEARCH WORK


DEDICATION

I dedicate this work to my parents, Kheriah and Ali.
To my wife, Mabroka, for her many years of love and support in our home and to our children Saleh and Rafiq who have waiting patiently until the completion of this research
To my brothers Ismail and Alhadi for their waiting and encouragement
Acknowledgments

I would like to express my deepest gratitude to my supervisor Puan Zarinah Mod. Kasirun for her encouragement, continuous support, advice and comments, throughout my research.

I am also greatly indebted to my previous supervisor Prof. Dr. Khairuddin Hashim for his guidance, encouragement, advice, review, and constrictive criticism throughout my research.

My special thanks go to Tawfiq, Nassrudien, Abddalsalam, Abdalbaset, Azhanni, Dr. Merghani for their comments and advice.

I also wish to express my sincere gratitude and thanks to my colleagues, Hanan, Raj, Martin, Ibrahim, Azizi, Zahied and his wife, Elshabani and all postgraduate students at FSKTM/UM.

I thank all my friends in University of Malaya Salam, Lajili, Ashraf, Mesbah, and others.

I also thank the whole personnel at Libyan People's Bureau in Kuala Lumpur for their support.

Last but not least, I want to thank the Dean Prof. Mashkuri and whole personnel at the FSKTM / UM for their full support.
ABSTRACT

Software risk management is still a new concept in software industry. In this research, existing approaches of software risk management are investigated. A survey for software risk management practices has been conducted, and its results are presented. Nevertheless, many inclinations have been determined in the existing approaches. In general, however, existing approaches tend to suffer from many shortcomings. For instance, they ignored or not covered well some important aspects like risk monitoring and documentation.

Since software risks increase with the growth of software developments. Therefore, seven risk items have been identified and proposed in this thesis to be added to the Top Ten risk items specified by Boehm. However, the work presented here introduces a new group of software risk management steps (technique), with emphasizes on risk documentation as an aspect could help to predict and avoid future risks. In addition, a mechanism to estimate software risks (probability and magnitude) has been presented.

Since many weaknesses have been detected in existing approaches prototype to tackle them was developed. This thesis describes the prototype, which is designed based on the proposed technique. Firstly, its requirement specification, analysis and design and implementation phases are discussed. The prototype has also been tested and validated.

The testing and validation results are discussed as well. The prototype comes out with many contributions and features (e.g. representing risk exposure with a line graph for monitoring purpose, risk documentation, probability and magnitude estimation, statistical data preparation) which are expanded in this thesis.
# TABLE OF CONTENTS

List of Figures ........................................................................................................ IX
List of Tables ........................................................................................................ XI

## CHAPTER ONE: GENERAL INTRODUCTION

1.1 Introduction ...................................................................................................... 1
1.2 Software Disasters .......................................................................................... 2
1.3 Basic Concept .................................................................................................. 3
1.4 Risk Monitoring ............................................................................................... 4
1.5 Software Risk Management History .................................................................. 5
1.6 Motivation ........................................................................................................ 6
1.7 Benefits of Risk Management .......................................................................... 7
1.8 Project Aims ..................................................................................................... 8
1.9 Metodology .................................................................................................... 9
1.10 Thesis Overview ............................................................................................ 9

## CHAPTER TWO: SOFTWARE RISK MANAGEMENT

2.1 Introduction .................................................................................................... 11
2.2 Theoretical Background ............................................................................... 12
  2.2.1 Risk Sources ............................................................................................ 12
  2.2.2 Likelihood / Potential / Probability ......................................................... 14
  2.2.3 Loss/Impact / Consequence / Magnitude ............................................... 15
  2.2.4 Software and Risk ................................................................................... 15
  2.2.5 Software Risks Categories and Types .................................................... 16
  2.2.6 Software Risk Management Concept .................................................... 17
    2.2.6.1 Software Risk Management Motivation ........................................ 18
    2.2.6.2 Narrative, Qualitative or Quantitative ........................................... 19
    2.2.6.3 Risk Exposure (RE) ......................................................................... 20
    2.2.6.4 Risk Reduction Leverage (RRL) ...................................................... 21
    2.2.6.5 Risk Reduction Options ................................................................. 21
  2.2.7 Software Risk Management Steps ......................................................... 22
    2.2.7.1 Boehm's Steps ............................................................................... 22
    2.2.7.2 Charette's Steps ............................................................................ 24
    2.2.7.3 Rakos's Steps ............................................................................... 25
    2.2.7.4 Jacobson's Steps ........................................................................... 26
    2.2.7.5 Fairley's Steps ............................................................................... 27
    2.2.7.6 Software Engineering Institute (SEI) Steps .................................. 28
    2.2.7.7 Risk Assessment and Mitigation Procedure (RAMP) Steps ......... 29
    2.2.7.8 Riskit Method Steps ...................................................................... 30
CHAPTER THREE: SOFTWARE RISK MANAGEMENT SURVEY

3.1 Introduction ............................................................................. 56
3.2 Prior Studies ........................................................................ 57
3.3 Research Approach ................................................................. 58
3.4 Survey Results ...................................................................... 58
  3.4.1 Top Risk Items Evaluation .................................................. 60
    3.4.1.1 Top Ten Risk Items ....................................................... 60
    3.4.1.2 Additional Top Seven Risks ........................................... 63
3.5 Discussion ............................................................................ 69
3.6 Conclusion ........................................................................... 70
CHAPTER FOUR: SOFTRISK ANALYSIS AND REQUIREMENTS DEFINITION

4.1 Introduction........................................................................................................... 71
4.2 Information Description....................................................................................... 71
  4.2.1 Problems and Motives................................................................................... 71
  4.2.2 General Requirements.................................................................................. 73
4.3 Functional and Behavioural Description............................................................. 75
  4.3.1 Identification, Estimation, and Documentation............................................. 75
    4.3.1.1 Risks’ Database (RskDB) Manager....................................................... 75
    4.3.1.2 Projects’ Risks File (PRSf) Manager.................................................... 77
    4.3.1.3 Probability and Magnitude Estimator................................................. 79
  4.3.2 Assessment and Prioritisation.......................................................................... 80
  4.3.3 Monitoring and Controlling.......................................................................... 81
    4.3.3.1 Monitoring........................................................................................... 81
    4.3.3.2 Controlling and Re-assessment......................................................... 81
  4.3.4 Statistics Preparation...................................................................................... 85
    4.3.4.1 Risks Threatens.................................................................................... 85
    4.3.4.2 Risks Frequency................................................................................... 85
    4.3.4.3 Risks Sorting....................................................................................... 85
    4.3.4.4 Risks Infection Impact......................................................................... 86
    4.3.4.5 Risks Similarity.................................................................................... 86
  4.4 Overview on SoftRisk Steps.............................................................................. 86
    4.4.1 Step 1: Risk Identification........................................................... 87
    4.4.2 Step 2: Risk Probability and Magnitude Estimation................................. 89
    4.4.3 Step 3: Risk Documentation ..................................................................... 89
    4.4.4 Step 4: Risk Assessment........................................................................... 89
    4.4.5 Step 5: Prioritisation and Highlighting Highest Ten Risks....................... 90
    4.4.6 Step 6: Monitoring (Graphical Representation)......................................... 90
    4.4.7 Step 7: Controlling and Reassessment.................................................... 90
    4.4.8 Step 8: Performing Statistical Operations and going back to step 1............ 91
  4.5 SoftRisk Implementation Requirements and Environment............................. 91
    4.5.1 The Hardware........................................................................................... 91
    4.5.2 The Software............................................................................................ 91
  4.6 Conclusion........................................................................................................... 92

CHAPTER FIVE: SOFTRISK DESIGN

5.1 Introduction.......................................................................................................... 93
5.2 Description of SoftRisk Design......................................................................... 93
  5.2.1 Risk Matrix.................................................................................................. 93
  5.2.2 SoftRisk Main Classes.................................................................................. 94
    5.2.2.1 SoftRiskStarter Class........................................................................... 95
    5.2.2.2 OperationsSelector Class.................................................................... 95
5.2.2.3 Risk_Documentation Class
5.2.2.4 Projects_Risks Class
5.2.2.5 Risk_Assessment_and_Prioritization Class
5.2.2.6 Monitoring_and_Controling Class
5.2.2.7 Graphic_Builder Class
5.2.2.8 Controlling Class
5.2.2.9 Prob_Mag_Estimation_Assistance Class
5.2.2.10 Prob_Mag_Preparation Class
5.2.2.11 Prob_Mag_Utilization Class
5.2.2.12 Statistical_Data_Preparation Class

5.2.3 SoftRisk Interaction Diagrams
5.2.4 Uder Interface Design
5.2.4.1 The Design of RskDB Data Entry/Retrieve Frame
5.2.4.2 The Design of PRSF Data Entry/Retrieve Frame
5.2.4.3 Estimation Assistance Utilization Frame Design (probability side)

5.3 Conclusion

6.1 Introduction
6.2 Development Environment
6.2.1 Software Used
6.2.2 Hardware Used

6.3 SoftRisk Components Description
6.3.1 Projects' Risks Handling
6.3.1.1 Specifying A Group of Risks
6.3.1.2 Selecting One of Project's Records
6.3.1.3 Adding Data
6.3.2 Risks Documentation
6.3.2.1 Adding Data to RskDB
6.3.2.2 Working on Previous Registered Records
6.3.3 Risk Assessment and Prioritization
6.3.4 Monitoring and Controlling
6.3.4.1 Selecting A Project
6.3.4.2 Monitoring Preparation
6.3.4.3 Graphic Builder
6.3.4.4 Risk Controlling
6.3.5 Statistical Data Preparation
6.3.5.1 Risks Threatens
6.3.5.2 Risks Frequency
6.3.5.3 Risks Sorting
6.3.5.4 Risk Infection
6.3.5.5 Risks Similarity

CHAPTER SIX: SOFTRISK IMPLEMENTATION

6.1 Introduction
6.2 Development Environment
6.2.1 Software Used
6.2.2 Hardware Used

6.3 SoftRisk Components Description
6.3.1 Projects' Risks Handling
6.3.1.1 Specifying A Group of Risks
6.3.1.2 Selecting One of Project's Records
6.3.1.3 Adding Data
6.3.2 Risks Documentation
6.3.2.1 Adding Data to RskDB
6.3.2.2 Working on Previous Registered Records
6.3.3 Risk Assessment and Prioritization
6.3.4 Monitoring and Controlling
6.3.4.1 Selecting A Project
6.3.4.2 Monitoring Preparation
6.3.4.3 Graphic Builder
6.3.4.4 Risk Controlling
6.3.5 Statistical Data Preparation
6.3.5.1 Risks Threatens
6.3.5.2 Risks Frequency
6.3.5.3 Risks Sorting
6.3.5.4 Risk Infection
6.3.5.5 Risks Similarity
6.3.6 Implementation Problems and Difficulties ........................................... 142
6.4 Conclusion ............................................................................................... 143

CHAPTER SEVEN: SOFTRISK TESTING AND VALIDATION

7.1 Introduction .............................................................................................. 144
7.2 Testing ....................................................................................................... 144
  7.2.1 Testing Case ........................................................................................ 144
    7.2.1.1 Initialization Data ........................................................................ 145
    7.2.1.2 Inspection Data ........................................................................... 147
  7.2.2 Testing Implementation ........................................................................ 150
    7.2.2.1 Risks’ Database Testing ............................................................... 150
    7.2.2.2 Projects’ Risks Testing ................................................................. 152
    7.2.2.3 Monitoring and Controlling Testing ............................................ 156
    7.2.2.4 Statistics Preparation Testing ...................................................... 159
  7.3 Validation .................................................................................................. 163
  7.4 Conclusion ............................................................................................... 167

CHAPTER EIGHT: CONCLUSION

8.1 Summary .................................................................................................... 168
8.2 Contributions ............................................................................................. 169
  8.2.1 Research Contributions ...................................................................... 169
  8.2.2 The Features of SoftRisk ................................................................. 170
8.3 Limitation and Future Perspective ............................................................. 172
  8.3.1 Risk Statistics ..................................................................................... 172
  8.3.2 Specialization ..................................................................................... 173
  8.3.3 Integration .......................................................................................... 173
  8.3.4 Risk Cost Estimation .......................................................................... 173

REFERENCES

APPENDICES

Appendix A: A Sample of Software Risk Management Questionnaire ................. A-1
Appendix B: Checklists of Probabilities and Magnitudes Estimation of Top Risks ...... B-1
Appendix C: A Sample of Validation Questionnaire ............................................ C-1
<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Word-To-Probability Relationships</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>Cost/Benefits of Risk Mitigation</td>
<td>18</td>
</tr>
<tr>
<td>2.3</td>
<td>Software Risk Management Steps (Boehm)</td>
<td>23</td>
</tr>
<tr>
<td>2.4</td>
<td>Impact Assessment</td>
<td>33</td>
</tr>
<tr>
<td>2.5</td>
<td>Spiral Model</td>
<td>36</td>
</tr>
<tr>
<td>2.6</td>
<td>Air Force's Risk Assessment (AFSC/AFLC 800-45) Matrix</td>
<td>38</td>
</tr>
<tr>
<td>2.7</td>
<td>SEI-Taxonomy Structure</td>
<td>40</td>
</tr>
<tr>
<td>2.8</td>
<td>Part of the Taxonomy-Based Questionnaire</td>
<td>41</td>
</tr>
<tr>
<td>2.9</td>
<td>Risk Severity Contours</td>
<td>47</td>
</tr>
<tr>
<td>2.10</td>
<td>Monitoring on a Weekly Basis</td>
<td>49</td>
</tr>
<tr>
<td>3.1</td>
<td>Software Risks Types</td>
<td>59</td>
</tr>
<tr>
<td>3.2</td>
<td>Reasons for Non Implementation of Risk Management Techniques</td>
<td>60</td>
</tr>
<tr>
<td>3.3</td>
<td>Top Ten Risks Items (Sorted Based on Respondents Prioritization)</td>
<td>63</td>
</tr>
<tr>
<td>3.4</td>
<td>Additional Seven Top Risks (Sorted Based on Respondents Prioritization)</td>
<td>69</td>
</tr>
<tr>
<td>4.1</td>
<td>SoftRisk Steps Diagram (Continuous inspection and monitoring)</td>
<td>88</td>
</tr>
<tr>
<td>5.1</td>
<td>Class and Relationships Notation</td>
<td>95</td>
</tr>
<tr>
<td>5.2</td>
<td>SoftRisk: Main Classes Diagram</td>
<td>96</td>
</tr>
<tr>
<td>5.3</td>
<td>Risk Assessment and Prioritization</td>
<td>98</td>
</tr>
<tr>
<td>5.4</td>
<td>Interaction Diagram Scenario-1 (Risk Documentation)</td>
<td>103</td>
</tr>
<tr>
<td>5.5</td>
<td>Interaction Diagram Scenario-2 (Projects' Risks Identification)</td>
<td>104</td>
</tr>
<tr>
<td>5.6</td>
<td>Interaction Diagram Scenario-3 (Monitoring and Controlling)</td>
<td>105</td>
</tr>
<tr>
<td>5.7</td>
<td>Interaction Diagram Scenario-4 (Statistical Operations)</td>
<td>106</td>
</tr>
<tr>
<td>5.8</td>
<td>RskDB Data Entry/Retrieve Frame Design</td>
<td>108</td>
</tr>
<tr>
<td>5.9</td>
<td>PRSF Data Entry/Retrieve Frame Design</td>
<td>109</td>
</tr>
<tr>
<td>5.10</td>
<td>A Probability Estimator Frame</td>
<td>110</td>
</tr>
<tr>
<td>6.1</td>
<td>SoftRisk Main Components</td>
<td>114</td>
</tr>
<tr>
<td>6.2</td>
<td>Projects' Risks Handling Components</td>
<td>116</td>
</tr>
<tr>
<td>6.3</td>
<td>Specifying Risks for Entering Purpose</td>
<td>117</td>
</tr>
<tr>
<td>6.4</td>
<td>Selecting One of Projects Records for Display, Update, or Delete</td>
<td>118</td>
</tr>
<tr>
<td>6.5</td>
<td>Projects' Risk Record Selection</td>
<td>119</td>
</tr>
<tr>
<td>6.6</td>
<td>Risk Magnitude Estimator</td>
<td>123</td>
</tr>
<tr>
<td>6.7</td>
<td>Risk Documentation Components Hierarchy</td>
<td>125</td>
</tr>
<tr>
<td>6.8</td>
<td>Specifying A Risk Record</td>
<td>128</td>
</tr>
<tr>
<td>6.9</td>
<td>Reduction Action Documentation</td>
<td>137</td>
</tr>
<tr>
<td>6.10</td>
<td>Diagram of Infected Projects Processing</td>
<td>139</td>
</tr>
<tr>
<td>7.1</td>
<td>Testing of RskDB Data Entry/Retrieve Frame</td>
<td>140</td>
</tr>
<tr>
<td>7.2</td>
<td>Risk-Code Checker</td>
<td>141</td>
</tr>
<tr>
<td>7.3</td>
<td>Probability and Magnitude Preparation Testing</td>
<td>152</td>
</tr>
<tr>
<td>7.4</td>
<td>Testing the Projects Code Detector</td>
<td>153</td>
</tr>
<tr>
<td>7.5</td>
<td>Testing the Risk Code Detector</td>
<td>154</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 2.1: Quantification of Performance Probability ............................................... 32
Table 2.2: The Existing Top Ten Risk Items ................................................................. 34
Table 2.3: Levels of Magnitudes and Guidelines .......................................................... 39
Table 2.4: Risk Factors in Software Development ......................................................... 42
Table 2.5: Measures for Risk Factors ........................................................................... 43
Table 2.6: RAMP Capability Levels ............................................................................. 44
Table 2.7: Checkbox for Risk Analysis ......................................................................... 45
Table 2.8: Risk Model Using Weighting Factors .............................................................. 46
Table 2.9: Computed Reference Points ......................................................................... 46
Table 2.10: Risk Severity Table .................................................................................... 47
Table 2.11: Risk Chart ................................................................................................. 51
Table 2.12: Comparison between Related Tools ............................................................. 54
Table 3.1: Reasons for Non Implementation of Risk Management Techniques ................ 59
Table 3.2: Existing Top Ten Risk Items ....................................................................... 61
Table 3.3: Top Ten Risk Items Evaluation ................................................................... 62
Table 3.4: Additional Top Seven Risk Items ................................................................. 64
Table 3.5: Additional Top Seven Risk Items Evaluation .............................................. 68
Table 4.1: A Sample of Probability and Magnitude Estimation Checklists .................... 80
Table 5.1: Risk Matrix Example ................................................................................... 94
Table 6.1: Bufferdata Example .................................................................................. 129
Table 6.2: BufferReady Example ................................................................................. 130
Table 7.1: A Sample of Risks' Database Initialization Data .......................................... 145
Table 7.2: Data sample of probability and magnitude estimator checklist .................... 146
Table 7.3: Codes and Risks Names .............................................................................. 147
Table 7.4: Sample of Fixed Data ................................................................................ 148
Table 7.5: Changeable Inspection Data ........................................................................ 149
Table 7.6: Validation Questionnaire ............................................................................ 164
Table 7.7: Summary of the questionnaire results ......................................................... 165
Table 8.1: Comparison with Previous Tools .................................................................. 172