METHODOLOGY FOR PRACTICE OF INFORMATION SECURITY IN SOFTWARE DEVELOPMENT COMPANIES

Edirisinhage Kasun Udara Jayasekara

(169111T)

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

METHODOLOGY FOR PRACTICE OF INFORMATION SECURITY IN SOFTWARE DEVELOPMENT COMPANIES

Edirisinhage Kasun Udara Jayasekara

(169111T)

The dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfillment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

……………………………….

Edirisinhage Kasun Udara Jayasekara

(Signature of the candidate) Date:

The above candidate has carried out research for the Masters thesis under my supervision.

……………………………….. ………………….

Dr Chandana Gamage Date

Signature of the Supervisor

COPYRIGHT STATEMENT

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

ABSTRACT

When modern organizations are considered, information is one of the most critical assets that need to be protected against external and internal threats. Since there is a massive increase in threats related to information technology applications, information security has become a significant factor. Moreover, information security ensures business continuity and reduce the risk of damage to an organization's reputation. Therefore, internal information security management is a critical factor. There are several factors which affect implementation of information security management. This research is focused on finding out a methodology for information security management in software development companies. To achieve objective information security governance, senior management support and organizational culture factors impact on information security management in software development companies are comprehensively studied. Furthermore, existing management models such as plan, do, check and act model, maturity models, etc., were analyzed to understand its applicability to information security management. An online questionnaire was developed based on three major factors identified during the literature review and shared with Associate technical leads, Technical leads, Software architects, Project managers, Delivery managers, Information Technology managers and Heads of IT in the software industry to represent the information security decision makers in an organization. Collected data was analyzed quantitatively using a statistical tool.

The research results have shown a strong positive relationship between information security governance and senior management support with information security management. Whereas Organizational culture has a very weak relationship with information security management. According to the research results, PDCA can be recommended to manage information security in Software development organizations.

Keywords: Information security, Information security governance, Information security management, Organizational culture, PDCA Model

ACKNOWLEDGEMENT

I wish to express my sincere gratefulness to Dr Chandana Gamage, for the great support, inspiration and guidance gave me to complete this research study as my research supervisor. This research study may not be possible unless his guidance and kindness offered to me. Then I have to express my sincere gratitude to Ms Jeeva Padmini for the support and the kindness offered to me throughout this study. I sincerely thank all the academic and non-academic staff of the University of Moratuwa who supported me throughout this time period.

I have to express my gratitude to all respondents from different IT organizations of Sri Lanka, for responding to my research questionnaire by spending their valuable time. Then I would like to be thankful to fellow students of my MBA program for great support offered me by sharing their knowledge.

Finally, I have to express my sincere thank to my parents and my loving wife Dr Upulsara Jayawardhana for helping me every way that they can.

TABLE OF CONTENTS

Declaration iii

copyright statement iiii

Abstract v

Acknowledgement v

Table of Contents vii

List of Figures ix

List of Tables x

List of Abbreviations xii

1. Introduction 1

1.1.Background 1

1.1.1. Motivation 3

1.1.2. Research Scope 3

1.2.Problem Statement 3

1.2.1. Research Objectives 4

1.2.2. Research Significance 4

2. Literature Review 5

2.1. Introduction 5

2.2. Independent Variables 6

2.2.1. Senior management support 6

2.2.2. Organizational culture 7

2.2.3. Information security governance 8

2.3. Information Security Management Models 9

2.3.1 PDCA Model 9

2.3.2 Maturity models 15

2.3.2.1. Capability Maturity Models 15

2.3.2.2. Capability Maturity Model Integration (CMMI) 15

2.3.2.3. Relationship between maturity models and the information security.... 16

2.4. Summary 17

3. Research Methodology 19

3.1.Introduction 19

3.2.Research Design 19

3.3.Conceptual Framework 20

3.4.Data Collection 23

3.5.Summary 23

4. Data Analysis 25

4.1.Introduction 25

4.2.Data Collection 25

4.2.1. Preliminary survey 25

4.2.2. Research survey 25
4.3. Reliability Analysis 26
4.3.1. Information security governance 26
4.3.1.1. Information security governance for employees 26
4.3.1.2. Information security governance for process 27
4.3.1.3. Information security governance reliability analysis 28
4.3.2. Senior management support 29
4.3.2.1. Operational support 29
4.3.2.2. Policy support 30
4.3.2.3. Senior management support reliability analysis 31
4.3.3. Organizational culture 32
4.3.3.1. Empowerment 32
4.3.3.2. Resistance to change 32
4.3.3.3. Organizational culture reliability analysis 33
4.3.4. Information security management 34
4.4. Demographic Analysis 36
4.4.1. Introduction 36
4.4.2. Current designation of the employee 36
4.4.3. Current working experience of the employee 37
4.4.4. Educational background of the employees 38
4.4.5. Number of employees in the company 39
4.5. Correlation Analysis 40
4.5.1. Pearson’s correlation 40
4.5.1.1. Senior management support vs. Information security management 40
4.5.1.2. Information security governance vs. Information security management 42
4.5.1.3. Organizational culture vs. Information security management 43
4.5.2. ANOVA Testing 43
4.5.2.1. Senior management support vs. Information security management 44
4.5.2.2. Information security governance vs. Information security management 44
4.5.2.3. Organizational culture vs. Information security management 44
4.6. Regression Analysis 45
4.6.1. Senior management support vs. Information security management 45
4.6.2. Information security governance vs. Information security management 46
4.6.3. Organizational culture vs. Information security management 47
4.7. Summary 48
4.7.1. Reliability test summary (Cronbach's Alpha value) 48
4.7.2. Inter item correlation analysis summary 49
4.7.2.1. Pearson Correlation summary 49
4.7.2.1. ANOVA table summary 49
4.7.3. Linear Regression Analysis 50
5. Recommendations and Conclusion 51
5.1. Introduction 51
5.2. Discussion of the Research Findings 51
5.3. Recommendations for Future Research 53

References 54

Appendix A: Online Survey Questionnaire 57

LIST OF FIGURES

Figure 1.1 Number of reported vulnerabilities between 1988 to 2018……….……. 2

Figure 2.1 General implementation of PDCA model……………………………… 12

Figure 2.2 Four-layer model for information security management ……………… 13

Figure 2.3 IS0 27001 establishment using PDCA model …………………………. 13

Figure 2.4 PDCA model for incremental approach …………………………...….. 14

Figure 3.1 Research methodology…………………………………………………. 19

Figure 3.2 Conceptual framework…………………………………………………. 21

Figure 3.3 Mapping diagram………………………………………………………. 22

Figure 4.1 Response frequency distribution with the time………………………… 25

Figure 4.2 Designations of the employees…………………………………………36

Figure 4.3 Current working experience of the employees……………………….… 37

Figure 4.4 Educational background of the employees………………………...… 38

Figure 4.5 Number of employees in the company…………………………………39

Figure 4.6 Direct comparison correlation between information security management and the senior management support…….……………………………... 41

Figure 4.7 Direct comparison correlation between information security management and the information security governance …………………………… 42

LIST OF TABLES

Table 2.1 Identified factors related to information security management…………..5
Table 2.2 Risk assessment plan ……………..…………………………………… 10
Table 2.3 Maturity models required to information security management……….. 16
Table 3.1 Mapping table for objectives, factors and questions…………………… 21
Table 4.1 Cronbach's alpha value representation …………………………………26
Table 4.2 Information security governance for employees……………………….. 26
Table 4.3 Case Processing summary for Information security governance for employees……………………………………………………………………… 27
Table 4.4 Reliability Statistics of Information security governance for employees.27
Table 4.5 Information security governance for process……………………………27
Table 4.6 Case Processing Summary for Information security governance for process………………………………………………………………………….. 27
Table 4.7 Reliability Statistics of Information security governance for process…. 27
Table 4.8 Case Processing Summary for information security governance……… 28
Table 4.9 Reliability Statistics for information security governance…………….. 28
Table 4.10 Information security governance…………………………………... 29
Table 4.11 Operational support………………………………………………... 29
Table 4.12 Case Processing Summary of Operational support…………………... 30
Table 4.13 Reliability Statistics of Operational support………………………… 30
Table 4.14 Policy support……………………………………………………… 30
Table 4.15 Case Processing Summary of Policy support………………………… 30
Table 4.16 Reliability Statistics of Policy support……………………………….. 30
Table 4.17 Case Processing Summary for senior management support………… 31
Table 4.18 Reliability Statistics for senior management support………………… 31
Table 4.19 Senior management support……………………………………….. 31
Table 4.20 Empowerment……………………………………………………… 32
Table 4.21 Case Processing Summary for Empowerment……………………….. 32
Table 4.22 Reliability Statistics for Empowerment……………………………… 32
Table 4.23 Resistance to change……………………………………………….. 32
Table 4.24 Case Processing Summary for Resistance to change………………… 33
Table 4.25 Reliability Statistics for Resistance to change……………………….. 33
Table 4.26 Case Processing Summary for organizational culture……………….. 33
Table 4.27 Reliability Statistics for organizational culture……………………… 33
Table 4.28 Organizational culture……………………………………………… 34
Table 4.29 Case Processing Summary for Information security management…… 34
Table 4.30 Reliability Statistics for Information security management………….. 34
Table 4.31 Information security management…………………………………… 34
Table 4.32 Designations of the employees……………………………………….. 36
Table 4.33 Current working experience of the employees……………………….. 37
Table 4.34 Educational background of the employees…………………………… 38
Table 4.35 Number of employees in the company……………………………….. 39
Table 4.36 Pearson's correlation……………………………………………….. 40
Table 4.37 Correlation between information security management and the senior management support………………………………………………………… 41

Table 4.38 Correlation between information security management and the information security governance……………………………………………… 42
Table 4.39 Correlation between information security management and the Organizational culture……………………………………………………….. 43
Table 4.40 ANOVA results comparison between senior management support vs. Information security management……………………………………………44
Table 4.41 ANOVA results comparison between Information security governance vs. Information security management………………………………………… 44
Table 4.42 ANOVA results comparison between organizational culture vs. Information security management……………………………………………44
Table 4.43 Model Summary comparison between senior management support vs. Information security management……………………………………………45
Table 4.44 Coefficients results comparison between senior management support vs. Information security management………………………………………….. 46
Table 4.45 Model Summary comparison between Information security governance vs. Information security management…………………………………………...46
Table 4.46 Coefficients results comparison between information security governance vs. Information security management………………………………...47
Table 4.47 Model Summary comparison between organizational culture vs. Information security management……………………………………………47
Table 4.48 Coefficients results comparison between organizational culture vs. Information security management……………………………………………48
Table 4.49 Reliability test summary……………………………….……………48
Table 4.50 Pearson Correlation summary…………………….……………….... 49
Table 4.51 ANOVA table summary……………………..…………………...49
Table 4.52 Coefficient table summary…………………………….……………….50

LIST OF ABBREVIATIONS

Abbreviation	**Description**
BDIM	Business Driven Information technology Management
BSC	Balanced Scorecard framework
CMMI	Capability Maturity Model Integration
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and related Technologies
CSI	Crime Scene Investigation
FBI	Federal Bureau of Investigation
IDEAL	Initiating, Diagnosing, Establishment, Acting and Learning
ISG	Information Security Governance
ISM	Information Security Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OC	Organizational Culture
OPM3	Organizational Project Management Maturity Model
PDCA	Plan, Do, Check and Act
QIP	Quality Improvement Paradigm
ROI	Return On Investment
SLASSCOM	Sri Lanka Association of Software and Service Companies
SMS	Seiner Management Support
SRE	Secure Requirement Engineering
SSE-CMM	System Security Engineering Maturity Model