ENHANCEMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM
BY EMBEDDING CORPORATE ETHICAL VIRTUE AS ETHICAL ISSUES
SOLUTION

NUR ZAFIRAH BINTI ABD HASHIM

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2015
This project report is dedicated to my lovely husband; Muhammad Iqbal Tariq and my parents; Abd Hashim, Rohani, Idris and Norliza and to my siblings for their endless support and encouragement.
ACKNOWLEDGEMENT

First and foremost, Alhamdulillah to my creator the Almighty. I would like to express heartfelt gratitude to my supervisor Prof Madya Dr Norafida Ithnin for her constant support during my study at UTM. She inspired me greatly to work in this project. Her willingness to motivate me contributed tremendously to our project. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor.

I also want to express my gratitude to my husband and family members for their endless support and gave me advice when I am needed.

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.
ABSTRACT

The effectiveness and successful of the Information Security (IS) can be influenced by many factors such as the human, process, technology and organizational. Hence, the Information Security Management System (ISMS) is an appropriate approach for handling and managing the information security. However, there are issues of an ethical among human and organizational cultures which affect the successful of the information security. This is because of only focusing on the technical aspect rather than human and organizational solution. The small implementing of the ethics within the information security management leads to leakage of the information in the organization. Thus, the information must be protected by highlight the important of the ethical to make the information valuable assets to the organization. Due to these issues, there are several ethical issues in information security management such as human factor as illegal behaviour and human error, the technology, the process of information security management as accountability and responsibility and also the management and organizational culture factors of information security. In this research, the PDCA is an approach used as the Information Security Management (ISM) which consist of the plan, do, check and act phase. In order to evaluate the enhancement of the ISMS process, the selected Corporate Ethical Virtue (CEV) component is embedded toward the processes as an ethical issues solution. The selected CEV components are Supportability, Clarity, Discussability, Transparency, Sanctionability, Feasibility and Congruency. The proposed of enhancement ISMS process by embedding CEV as an ethical issues solution is validate by the credibility experts.
ABSTRAK

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xiv</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xv</td>
</tr>
<tr>
<td>LIST OF APPENDIXES</td>
<td></td>
<td>xvi</td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 Introduction                  1  
1.2 Problem Background            2  
1.3 Problem Statement             3  
1.4 Project Aim                   3  
1.5 Objectives of the Project     4  
1.6 Project Scope                 4  
1.7 Significant of the Project    4  
1.8 Organization of Report        5  

## 2 LITERATURE REVIEW

2.1 Introduction                  6  
2.2 Information Security          7  
2.2.1 Information Security Control 8
2.2.2 Factor Influence in Information Security 11
  2.2.2.1 Organizational Factor 11
  2.2.2.2 Human Factor 12
  2.2.2.3 Technological Factor 13
2.3 Information Security Management System (ISMS) 13
  2.3.1 Information Security Management Standard 18
  2.3.2 Process of Information Security Management System (ISMS) 21
  2.3.3 Issues in ISMS 23
2.4 Ethical issues 26
  2.4.1 Ethical Issues in Information Security 27
  2.4.2 Information Ethics 32
  2.4.3 Ethical Policy 34
  2.4.4 Ethical Cultures 35
2.5 Definition of CEV 37
  2.5.1 Purpose of CEV 37
  2.5.2 Component of CEV 38
  2.5.3 Strategic in CEV 41
  2.5.4 Benefit of CEV 42
2.6 Conclusion 42

3 METHODOLOGY
  3.1 Introduction 43
  3.2 Operational Framework 43
  3.3 Phase 1 47
  3.4 Phase 2 48
  3.5 Phase 3 49
  3.6 Structure of Questionnaire 49
  3.7 Conclusion 51

4 ISMS ENHANCEMENT WITH CEV
  4.1 Introduction 52
4.2 The Relation of ISMS and Ethical Issues 52
4.3 The Relation of CEV and Ethical Issues 55
4.4 The Relation of ISMS Process, CEV and Ethical Issues 59
4.5 The Selection 61
4.6 Process Enhancement 64
   4.6.1 Description Scope of ISMS 64
      4.6.1.1 Description Scope of ISMS with Clarity 65
   4.6.2 Definition of Security Policy 65
      4.6.2.1 Definition of Security Policy with Supportability 65
   4.6.3 Risk Assessment 66
      4.6.3.1 Risk Assessment with Feasibility 67
   4.6.4 Risk Management 67
   4.6.5 Control Selection 68
   4.6.6 Statement of Applicability 68
   4.6.7 Operate and Implement ISMS 68
      4.6.7.1 Operate and Implement ISMS with Discussability 69
      4.6.7.2 Operate and Implement ISMS with Congruency 69
      4.6.7.3 Operate and Implement ISMS with Sanctionability 69
   4.6.8 Review and Monitor ISMS 70
      4.6.8.1 Review and Monitor ISMS with Transparency 70
      4.6.8.2 Review and Monitor ISMS with Congruency 71
      4.6.8.3 Review and Monitor ISMS with Sanctionability 71
   4.6.9 Maintain and Improve ISMS 71
      4.6.9.1 Maintain and Improve ISMS with Congruency 72
4.6.9.2 Maintain and Improve ISMS with Sanctionability 72

4.7 Proposed Enhancement Validation 72

4.8 Conclusion 72

5 ISMS ENHANCEMENT WITH CEV RESULT AND ANALYSIS

5.1 Introduction 74

5.2 Analysis of Enhancement Process as Ethical Solution 75

5.2.1 Description Scope of ISMS with Clarity 77

5.2.2 Definition of Security Policy with Supportability 80

5.2.3 Risk Assessment with Feasibility 82

5.2.4 Operate and Implement ISMS with Discussability 84

5.2.5 Review and Monitor ISMS with Transparency 85

5.2.6 Maintain and Improve ISMS with Congruency 87

5.2.7 Maintain and Improve ISMS with Sanctionability 89

5.3 The Summary Analysis of the Expert’s Feedback 91

5.4 The Contribution of Embedding CEV as the Ethical Solution 92

5.5 The Enhancement of ISMS Process by Embedding CEV Component as Ethical Issues Solution 99

5.6 Conclusion 102

6 DISCUSSION AND CONCLUSION

6.1 Introduction 103

6.2 Achievement of the Project 103

6.2.1 First Achievement 104

6.2.2 Second Achievement 104

6.2.3 Third Achievement 104

6.3 Project Constraint 105
6.4 Future Work 105
6.5 Conclusion 106

REFERENCES 107
APPENDIXES 112
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>The Details of the Information Security Control</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Description of ISMS</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>The Simplification of ISMS Components</td>
<td>17</td>
</tr>
<tr>
<td>2.4</td>
<td>The Historical of ISMS Standard</td>
<td>19</td>
</tr>
<tr>
<td>2.5</td>
<td>Timeline of the Origin ISO 27001</td>
<td>19</td>
</tr>
<tr>
<td>2.6</td>
<td>PDCA Cycle</td>
<td>21</td>
</tr>
<tr>
<td>2.7</td>
<td>The Details of ISMS Process</td>
<td>23</td>
</tr>
<tr>
<td>2.8</td>
<td>The Description of Ethical Elements</td>
<td>25</td>
</tr>
<tr>
<td>2.9</td>
<td>The Ethical Issues in Information Security</td>
<td>27</td>
</tr>
<tr>
<td>2.10</td>
<td>The Description of Ethical Issues</td>
<td>29</td>
</tr>
<tr>
<td>2.11</td>
<td>Discussion between Ethic and Information Ethic</td>
<td>33</td>
</tr>
<tr>
<td>2.12</td>
<td>The Element of Ethical Policy</td>
<td>34</td>
</tr>
<tr>
<td>2.13</td>
<td>Detailed of CEV</td>
<td>39</td>
</tr>
<tr>
<td>3.1</td>
<td>Phases in Research Methodology</td>
<td>44</td>
</tr>
<tr>
<td>3.2</td>
<td>Description of Research Methodology</td>
<td>46</td>
</tr>
<tr>
<td>4.1</td>
<td>Matrix Mapping of ISMS Process and Ethical Issue</td>
<td>53</td>
</tr>
<tr>
<td>4.2</td>
<td>Matrix mapping of the CEV and Ethical Issues</td>
<td>56</td>
</tr>
<tr>
<td>4.3</td>
<td>The Relationship of ISMS Process, CEV and Ethical Issues</td>
<td>60</td>
</tr>
<tr>
<td>4.4</td>
<td>The Selection of CEV Component</td>
<td>62</td>
</tr>
<tr>
<td>5.1</td>
<td>List of Experts</td>
<td>75</td>
</tr>
<tr>
<td>5.2</td>
<td>Expert’s Feedback on Embedding Clarity</td>
<td>78</td>
</tr>
<tr>
<td>5.3</td>
<td>Expert’s Feedback for Embedding Supportability</td>
<td>80</td>
</tr>
<tr>
<td>5.4</td>
<td>Expert’s Feedback for Risk Assessment Embed with Feasibility</td>
<td>82</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.5</td>
<td>Expert’s Feedback on Discussability</td>
<td>84</td>
</tr>
<tr>
<td>5.6</td>
<td>Expert’s Feedback of the Transparency</td>
<td>86</td>
</tr>
<tr>
<td>5.7</td>
<td>Expert’s feedback of the Congruency</td>
<td>88</td>
</tr>
<tr>
<td>5.8</td>
<td>Expert’s feedback of the Sanctionability</td>
<td>90</td>
</tr>
<tr>
<td>5.9</td>
<td>The Contribution of Each Selected Component of CEV</td>
<td>93</td>
</tr>
</tbody>
</table>
### LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Connection of Organizational Factor</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>The ISO Standards in Implementing the ISMS</td>
<td>20</td>
</tr>
<tr>
<td>2.3</td>
<td>Lifecycle of PDCA Model in ISMS</td>
<td>22</td>
</tr>
<tr>
<td>2.4</td>
<td>Layer of Ethical Culture</td>
<td>36</td>
</tr>
<tr>
<td>3.1</td>
<td>Research Methodology Framework</td>
<td>45</td>
</tr>
<tr>
<td>5.1</td>
<td>Final Process of Embedded of CEV component in ISMS Process</td>
<td>100</td>
</tr>
</tbody>
</table>
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>ABBREVIATIONS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEV</td>
<td>Corporate Ethical Virtue</td>
</tr>
<tr>
<td>ISM</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>IS</td>
<td>Information Security</td>
</tr>
<tr>
<td>SoA</td>
<td>Statement of Applicability</td>
</tr>
</tbody>
</table>
LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>ISMS PROCESS (ISO 27001)</td>
<td>112</td>
</tr>
<tr>
<td>B</td>
<td>The List of Experts</td>
<td>116</td>
</tr>
<tr>
<td>C</td>
<td>Expert’s Feedback</td>
<td>117</td>
</tr>
<tr>
<td>D</td>
<td>Expert’s Approval</td>
<td>132</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, information flow in the organization may create by the employees by exchange any of related information of the organization. Hence, the security of the information is the most critical issues that need to be stress by the organization in order to exchange or sharing the information.

But, most of the solution of managing the information only based on the technical solution rather than others factor such as ethical issues as human factor towards the information security. The ethical issues may give the impact or influenced on the successful in the information security. Unfortunately, according to some researcher, lack of implementation of the ethical issues towards the information security management leads to untrusted and unsecure of the information in the organization. Thus, the information must be protected by highlight the important of the ethical to make the information valuable assets to the organization.
1.2 Problem Background

The information security management is defined as a set of policy that concern information security elements such as confidentiality, integrity and availability of the information (Kruger and Kearney, 2006). But nowadays, the lacked of securing the information is much critical because most of the process or the approaches within the information security management more focus on the technical solution.

In fact, according to CSI computer crime and security survey stated that around 52% still infected with the virus even though 98% of the user have the antivirus on the computer (Richardson, 2007). This shows that, if only the technical part is working to secure the information, the individual should take the risk of leaking the security of the information. Indeed, to mitigate this problem, the ethics elements need to be involved in the information security management system process to enhance the security of the information.

Another issue of information security in the ethical behavior is related to the right behavior. The survey was stated that 62% of the employee was monitoring others employee’s email and internet usage (Electronic policies and practice survey, 2001). This shows that the lacking of the internet behavior that related in ethical issues give impact on the information and employees trusted. Besides that, based on the Information security breaches survey stated that protecting of the customer information is the most importance for security that contain of 28% while 19% of preventing outages and downtime in the Internet worm attacks (Potter & Beard, 2010)

Information security management system (ISMS) is an approach to handle the information security. However, the approach mostly used is focusing on the technical approach for example developing the policy rather than ethical solution. Thus, to minimize the issues, some solutions on the technical and ethical solution can be balance
towards to secure the information. Other than that, the research of the ethical issues in the information security is investigated the solution to enhance the information security.

The Corporate Ethical Virtue (CEV) is a measurement model of the ethical culture of the organization. The CEV is an approach of normative formulates of criteria for the ethical culture in the organizations (Muel Kaptein, 2008). Thus, in order to enhance the information security management system (ISMS) process which may help the organization to secure and manage the information as the ethical solution within in the organization among employee, customer or stakeholder.

1.3 Problem Statement

Ethical issues influence the employee’s behaviors, organizational cultures and processes towards the information, customer or stakeholder as the valued assets in the organization. Others than that, ethic elements that implement will makes the information more secure in privacy of the information and benchmark to evaluate the behavior of the employee. Unfortunately, information security is more focus on the technical solution rather than ethical solutions and lacking of implementing the ethical issues in the organization leads to information's leaked. As a consequence, both organization and the employee are open to the potential threat such as privacy breach, low awareness among committees and untrusted towards the information's goal.

1.4 Project Aim

The aim of this project is to propose of embedding corporate ethical virtue in the information security management system process by using the PDCA approach as the ethical issues solution.
1.5 Objectives of the Project

There are three objectives in this project. The objectives are:

i. To study the ISMS process and CEV component in managing ethical solution in information security and analyzed current ISMS process and CEV component.
ii. To propose an ethical solution by embedding the CEV components to enhancing the ISMS process.
iii. To evaluate the enhancement of the ISMS process as an ethical issues solution by selecting CEV components in the information security.

1.6 Project Scope

The scopes of this project are:

i. This research is focus on the ISMS process as PDCA approach.
ii. This research stress on the CEV component to solved the possible ethical issues of the information security in the ISMS process.
iii. The enhancement in the ISMS process is by evaluation from the credible experts based on the distributed questionnaire.

1.7 Significant of the Project

The information security should focus not only on the technical part, but also need to focus on the human behavior or attribute to make the information more secure and effective to the organization. This is because the human factors influences in the
successfully of the information. Thus, the management and individual with high of ethics should take action to prevent breach of the information from happen.

1.8 Organization of Report

The report consists of six chapters. The description of each chapter is details in following sentences. Chapter 1 discussed about overview of the study, problem background, problem statement, aim of the project, objectives and scope. Chapter 2 consists of the literature review related in research area. The focus is on ISMS process, information security and ethical issues. Chapter 3 include of research methodology used in this project. Chapter 4 is stress on the process enhancement of the ISMS process with the selected CEV components. The analysis and result of this research is concluded in the Chapter 5. The discussion and conclusion of this project is on Chapter 6.
REFERENCES


Treviño, L., & Weaver, G. (2003). Managing ethics in business organizations:


