UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

AUTHOR’S FULL NAME : TEOH KAI WEI
TITLE : RISK MANAGEMENT TOOL USING OCTAVE APPROACH (PHASE 1)
ACADEMIC SESSION : 2008/2009

I declare that this thesis is classified as:

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1972)*
☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*
√ OPEN ACESS I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:
1. The thesis is the property of Universiti Teknologi Malaysia reserves the right as follows:
2. The library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

__________________________________
SIGNATURE

__________________________________
SIGNATURE OF SUPERVISOR

PERMANENT ADDRESS: NAME OF SUPERVISOR:
NO 16, JALAN HARMONI 1, DR. NORAFIDA BT ITHNIN
TAMAN HARMONI,
86200 SIMPANG RENGGAM , JOHOR

Date: 05 MAY 2009 Date: 05 MAY 2009

NOTES : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.
“I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of the degree of Bachelor of Science (Computer Science)”.

Tandatangan : ______________________
Nama Penyelia : DR. NORAPIDA BT ITHNIN
Tarikh : 05 MAY 2009
RISK MANAGEMENT TOOL USING OCTAVE APPROACH (PHASE 1)

TEOH KAI WEI

A project report submitted in partial fulfillment of the Requirements for the award of the degree of Bachelor of Science (Computer Science)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MAY, 2009
DECLARATION

I declare that this thesis entitled “Risk Management Tool Using Octave Approach (Phase 1)” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ........................................
Name : TEOH KAI WEI
Date : 05 MAY 2009
Specially dedicated to my beloved parents
For all their endless moral and financial support

To all my friends
Thanks for accompany me and help me to solve the problems that I faced

To the special one
Thanks for the caring, concern and moral support form you.
ACKNOWLEDGEMENT

I would like to take this opportunity to thank PSM supervisor, Dr. Norafida bt Ithnin for accepting me as her PSM student and her guidance during the period of developing this project.

I’m also very grateful to my lecturers, friends and also panels who always help me when I needed them and give me comment to correct my system. Without them, I can not finish this project smoothly.

Last but not least, I would like to thank all of them again.
ABSTRACT

The Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) is a framework for identifying and managing information security risks. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. This project is concern on converting manual sheet document into a system. Computer now is an essential for every company, so to convert the approach into a system will only bring more convenience for organization. This project is to measure current organizational security practices and provides a basis for developing security improvement strategies and risk mitigation plans. With this system, organization can design and implement a protection strategy more often to reduce the overall risk exposure of its information assets.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENT</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURE</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLE</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>LIST OF APPENDICES</td>
<td>xiv</td>
</tr>
</tbody>
</table>

## I  INTRODUCTION

1.1 Introduction  
1.2 Problem Background  
1.3 Project Aim  
1.4 Project Objective  
1.5 Project Scope  
1.6 Project Importance  
1.7 Summary

## II  LITERATURE REVIEW

2.1 Introduction  
2.2 Information Security  
2.3 Risk Management
2.4 Risk Analysis 10

2.4.1 Fault Tree Analysis, Failure Mode Effect Analysis 11

2.4.2 PRA Extensions or Modifications 12

2.4.3 Attack Trees and Vulnerability Trees 13

2.5 Existing Risk Management Methodologies 14

2.5.1 SSE-CMM Model 14

2.5.2 COBIT Model 18

2.5.3 NIST Model 20

2.5.4 ISM3 Model 21

2.5.5 CRAMM Model 23

2.5.6 SPMM Model 25

2.6 OCTAVE Model 27

2.6.1 Three Aspects – Three Phases 28

2.6.2 Principles of OCTAVE 29

III METHODOLOGY 32

3.1 Introduction 32

3.2 Project Methodology 32

3.2.1 Planning Stage 34

3.2.2 Analyzing Phase 34

3.2.3 Design Phase 34

3.2.4 Development Phase 35

3.2.5 Testing and Evaluation Phase 35

3.2.6 Advantages of Prototyping 35

3.2.7 Disadvantages of Prototyping 36

3.3 System requirements analysts 38

3.3.1 Hardware Requirements 37

3.3.1.1 Hardware Requirements for
VI       DISCUSSION AND CONCLUSION  56
6.1     Introduction              56
6.2     Achievements             56
6.3     Challenges               57
6.4     Expectation              57
6.5     Summary                  58

REFERENCES  59
APPENDICES  61

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>SSE-CMM Capability Levels</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>SSE-CMM Appraisal Process</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>SSE-CMM Capability Levels</td>
<td>17</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.4</td>
<td>COBIT Maturity Model</td>
<td>18</td>
</tr>
<tr>
<td>2.5</td>
<td>ISM3 Maturity Model</td>
<td>21</td>
</tr>
<tr>
<td>2.6</td>
<td>CRAMM Process</td>
<td>24</td>
</tr>
<tr>
<td>2.7</td>
<td>OCTAVE Process</td>
<td>28</td>
</tr>
<tr>
<td>2.8</td>
<td>Principles of OCTAVE</td>
<td>31</td>
</tr>
<tr>
<td>3.1</td>
<td>Process flow of an application design in evolutionary prototyping.</td>
<td>33</td>
</tr>
<tr>
<td>4.1</td>
<td>System Architectural Design</td>
<td>40</td>
</tr>
<tr>
<td>4.2</td>
<td>Use case diagram for admin</td>
<td>41</td>
</tr>
<tr>
<td>4.3</td>
<td>Use case diagram for Analyzer</td>
<td>41</td>
</tr>
<tr>
<td>4.4</td>
<td>Sequence diagram for delete data</td>
<td>43</td>
</tr>
<tr>
<td>4.5</td>
<td>Sequence diagram for update data</td>
<td>44</td>
</tr>
<tr>
<td>4.6</td>
<td>Sequence diagram for insert data into database</td>
<td>45</td>
</tr>
<tr>
<td>4.7</td>
<td>Sequence diagram of creating a risk management plan</td>
<td>46</td>
</tr>
<tr>
<td>4.8</td>
<td>Database of registered user</td>
<td>47</td>
</tr>
<tr>
<td>4.9</td>
<td>Database of Asset Group Worksheet</td>
<td>47</td>
</tr>
<tr>
<td>4.10</td>
<td>Database of Questionnaire</td>
<td>48</td>
</tr>
<tr>
<td>4.11</td>
<td>Interface design for the worksheets</td>
<td>49</td>
</tr>
<tr>
<td>4.12</td>
<td>Interface design for the login page</td>
<td>49</td>
</tr>
<tr>
<td>4.13</td>
<td>Interface of Log out page</td>
<td>50</td>
</tr>
<tr>
<td>5.1</td>
<td>Database Connection</td>
<td>53</td>
</tr>
<tr>
<td>5.2</td>
<td>Login</td>
<td>54</td>
</tr>
<tr>
<td>5.3</td>
<td>Insert of data</td>
<td>55</td>
</tr>
<tr>
<td>C1</td>
<td>Login page</td>
<td>65</td>
</tr>
<tr>
<td>C2</td>
<td>Page of login error</td>
<td>65</td>
</tr>
<tr>
<td>C3</td>
<td>Admin page</td>
<td>66</td>
</tr>
<tr>
<td>C4</td>
<td>Analysis form page</td>
<td>67</td>
</tr>
<tr>
<td>C5</td>
<td>Area of concern worksheet</td>
<td>68</td>
</tr>
<tr>
<td>C6</td>
<td>Survey Form</td>
<td>69</td>
</tr>
<tr>
<td>C7</td>
<td>Intro page</td>
<td>70</td>
</tr>
</tbody>
</table>
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>SSE-CMM Capability Levels</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Levels of COBIT Maturity Model</td>
<td>19</td>
</tr>
<tr>
<td>2.3</td>
<td>Levels of NIST Maturity Model</td>
<td>20</td>
</tr>
<tr>
<td>2.4</td>
<td>Levels of ISM3 Maturity Model</td>
<td>22</td>
</tr>
<tr>
<td>2.5</td>
<td>SPMM: General outline of the security</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>SPMM: Sample elements from security maturity model</td>
<td>26</td>
</tr>
<tr>
<td>2.7</td>
<td>SPMM: Sample of a quality measure from security maturity model</td>
<td>27</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>Gantt Chart</td>
<td>64</td>
</tr>
<tr>
<td>B</td>
<td>User Manual</td>
<td>67</td>
</tr>
</tbody>
</table>
Security is the condition of being protected against danger or loss. In the general sense, security has similar concept with safety. The nuance between the two words is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security. The word "security" in general usage is synonymous with "safety," but as a technical term "security" means that something not only is secure but that it has been secured. In telecommunications, the term security has the following meanings. Firstly, a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. Secondly, With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. Thirdly, measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. In the corporate world, various aspects of security were historically addressed separately, notably by distinct and often noncommunicating departments for IT security, physical security, and fraud prevention.
Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk. A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

1.2 Problem background

Today there is a greater recognition of the interconnected nature of security requirements, an approach variously known as holistic security, "all hazards" management, and other terms. Inciting factors in the convergence of security disciplines include the development of digital video surveillance and the digitization and networking of physical control systems. Greater interdisciplinary cooperation is further evidenced by the February 2005 creation of the Alliance for Enterprise Security Risk Management, a joint venture including leading associations in security (ASIS), information security (ISSA, the Information Systems Security Association), and IT audit (ISACA, the Information Systems Audit and Control Association). Security management is a broad field of management related to asset management, physical security and human resource safety functions. It entails the identification of
an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.

Therefore, organization need some tool to improve their security management. Management tools such as information classification, risk assessment and risk analysis are used to identify threats, classify assets and to rate system vulnerabilities. Risk management is a kind of management tool and also a structured approach to managing uncertainty related to a threat, a sequence of human activities including: risk assessment, strategies development to manage it, and mitigation of risk using managerial resources. The objective of risk management is to reduce different risks related to a preselected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. On the other hand it involves all means available for humans, or in particular, for a risk management entity (example: person, staff, organization). So, an effective risk management process is an important component of a successful IT security program. The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

As a conclusion, Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.
1.3 Project aim

The aim of this project is to develop risk management tool that uses OCTAVE method to help organization to measure current organizational security practices and provides a basis for developing security improvement strategies and risk mitigation plans.

1.4 Objective

Below is the objectives of the project:

i. To study, analysis and understand about existing risks management approach and method.
ii. To design and develop a system using risks management method.
iii. To test the functionality of the risk management tool with real data.

1.5 Scope

Below is the scope for the project:

i. The selected risk management approach is OCTAVE method.
ii. Only phase 1 of the Octave will completely be done.
iii. The selected language to create this system is Macromedia Dreamweaver and Sql to be the database.
iv. Test the system with the selected end users.
1.6 The importance of the project

This project may help to reduce the time that taking in identified the levels of risk. Because of that organization can do the identification more fluently. To done risk identification in document form will taking more time and this make organization can not check their operation system very often. This project also makes the risk analysis become more convenient and easy to be done. At the same time, workers that involve in the job can be reduces and the cost as well.

1.7 Summary

In this chapter, discuss about what is the objective, background of study, and the problem background. At the same time, reason why an organization need risk management tool, the importance of the risk management, benefits of the risk management tool, and lost that lead risk also included in this chapter.
CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Information as a concept has a diversity of meanings, from everyday usage to technical settings. Generally speaking, the concept of information is closely related to notions of constraint, communication, control, data, form, instruction, knowledge, meaning, mental stimulus, pattern, perception, and representation. In this chapter will include information security, organization information security, information system security, risk management and some existing method of risk management also introduce about my selected method of risk management approach.

2.2 Information Security

Information security also called "infosec," is the preservation of secrecy and integrity in the storage and transmission of information. Whenever information of any sort is obtained by an unauthorized party, information security has been
Breached. Breaches of information security can be divided into five basic classes, interception of messages, theft of stored data, information sabotage, spoofing, and denial of service. Individual computer experts that known as hackers, intelligence agencies, criminals, rival businesses, disgruntled employees, and other parties may all seek to breach information security. All these parties, plus law-abiding private individuals who wish to guard their privacy and protect themselves from identity theft, also have an interest in preserving information security.

Messages and secrets have been subject to interception and theft ever since the invention of writing, but the modern situation is especially challenging. Electronic storage, processing, and transmission of information are now ubiquitous in the developed world, creating novel vulnerabilities. People are authorized to withdraw cash or purchase products on the basis of a piece of information (password or credit card number); trade secrets and business plans are electronically transmitted around the globe. In the U.S., over 95% of military and intelligence communications pass through network facilities owned by private carriers like telephone system. Private speech may be broadcast locally by a mobile or cellular telephone or transmitted digitally over a network that can be tapped in numerous locations; databases full of confidential data reside in computers that can be accessed, perhaps illegally, by other computers communicating through networks; and so on. Information security or insecurity is a pervasive fact of modern life.

There are many tools for increasing information security, including software that scans for computer viruses or prevents unauthorized intrusions into computer systems from the networks; password systems of all sorts; physical access security for computers, discs, credit cards, and other objects containing sensitive information; and encryption of messages and of databases. While all these tools are important to the conduct of business by a large business or government department, passwords and encryption are probably the most important.

Passwords have the advantage of being simple to use. They are not, however, capable by themselves of providing a high level security for large numbers of users. First, most users are asked to supply passwords for many different systems: banking, shopping, e-mail, and so forth. This tempts users to choose short passwords (which
are easier to remember but also easier to guess, therefore weaker) and to use the same password for more than one system (causing a domino effect if a password is guessed).

Cryptography, the process by which raw message information (plaintext) is mapped or encrypted to a scrambled form (ciphertext) before transmission or storage, then mapped back to its original form again (decrypted) when an authorized party wishes to read the plaintext is arguably the ultimate tool of information security. High-quality cryptographic systems that are breachable (if at all) only by resource-rich groups like the U.S. National Security Agency are widely available to businesses, governments, and private individuals. Appropriate cryptography can virtually guarantee the security of messages in transit and of information in databases; it can also, through "authentication," act as a super-password system whereby the identity of a would-be user (or information service supplier) can be positively confirmed. Cryptography has the disadvantages of added complexity, higher cost, and system slowdown.

Cryptography is also politically controversial, despite, or rather, because of its technical power. Governments, corporations, private individuals, and private groups have both legitimate and, occasionally, illegitimate motives for information security. Law-abiding persons and groups, or those rebelling against repressive laws, wish to be secure from surveillance by governments; criminals, terrorists, and the like also wish to be secure from surveillance by governments; government agents who are committing crimes wish to avoid public exposure; and so forth. It is generally advantageous to all parties, whether their activities are legitimate or illegitimate in whatever sense, to advocate maximum privacy for their own activities; it is generally advantageous to governments to advocate, in addition, maximum transparency for everyone else. Thus, for example, the U.S. government has sought (with little success) to prevent the spread of high-quality encryption algorithms, such as Pretty Good Privacy, outside the U.S., and inside the country has sought to establish voluntary compliance with "escrowed" cryptography systems. In such systems a government agency stores copies of cryptographic keys that enable it to decrypt communications between private parties using the system. In theory, these escrowed keys would be released to police or other government agents only when the
court system had determined that there was a legitimate law enforcement or national-security need to do so. Because such systems allow for third-party access to encrypted information by design, they are intrinsically less secure than a non-escrowed cryptography system, and therefore predictably unpopular with the private sector.

2.3 Risk Management

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The DAA or system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family’s safety, a fundamental “mission” need. The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential
2.4 Risk Analysis

Quantitative risk analysis methods fall under the broad category of probabilistic risk assessment (PRA). A generally accepted definition of PRA is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. Although PRA technically includes the risk identification phase, it does not provide the guidance of methods like HHM, but rather assumes the designer can identify the risks. PRA includes all fault/attack (FTA) tree analyses, event tree analysis (ETA), failure mode and effect analysis (FMEA) or failure mode effect and criticality analysis (FMECA), and cause/consequence analysis (CCA), as well as methods that use directed graphs and logic diagrams (Henley and Kumamoto, 1996). Most other methods are extensions or combinations of these. Many of the tools mentioned earlier incorporate these methods to varying degrees.

Risk is characterized by the severity (or magnitude) of an adverse consequence that can result from an action and the likelihood of occurrence of the given adverse consequence. In probabilistic risk assessment, consequences are expressed numerically and their likelihoods of occurrence are expressed as probabilities or frequencies. Determining risk is generally accepted as answering the 3 questions: What can go wrong? How likely is it? What are the consequences? (Kaplan and Barrick, 1981). In PRA, these are answered by developing a set of scenarios or initiating events to answer what can go wrong, then evaluating the probability of the these scenarios, and finally estimating their consequences. The PRA ultimately presents a set of scenarios, frequencies, and associated consequences developed in a way to make informed decisions. RPA quantifies “risk metrics”, a term that refers to a consequence-oriented figure of merit, such as the probability of the top event (Stamatelalos, 2002). Determination of needed basic event probabilities is the most difficult task in applying this technique. Many references explain all aspects of PRA in great detail (Stamatelalos, 2002, Henley and Kumamoto, 1996).
2.41 Fault Tree Analysis, Failure Mode Effect Analysis

FTA (fault tree analysis), (Vesely, et al, 2002), is a deductive, failure-based approach. It starts with an undesired event, and then deduces event causes using a systematic backward reasoning process. A fault tree is constructed as a logical

Illustration of the events and their relationships necessary and sufficient to result in the undesired (top or root) event. The symbols used indicate the type of events and relationships involved such as AND gates (output of gate occurs if all inputs occur) and OR gates (output of gate occurs if any of the inputs occur). The fault tree displays the stepwise cause resolution using formal logic symbols. To evaluate the fault tree and calculate a top event probability, it has to be transformed into an equivalent set of logic equations. By successive substitution, each gate event is expressed in terms of basic events. The qualitative results obtained from FTA are “minimal cut sets”, the smallest combination of basic events that result in the top event (fault). Each minimal cut set is a combination of basic events. The set of minimal cut sets for the top event represents all the ways that basic events can cause the fault or top event. Quantification of FTA happens when top event probability is determined from basic event information by assigning probabilities to the basic events. Uncertainties in any quantified result can be determined. These top event probabilities can be used to calculate risk in financial or other terms. Several importance measures can be calculated to determine the change in the risk metric of interest such as the change in the top event probability when a basic event probability is set to zero (Stamatelalos, 2002).

The basic difference between FTA and inductive methods is the direction of the analysis. FTA starts with the undesired event and traces backward to causes, whereas inductive methods start with an initiating event and trace forward to consequences. Thus, FTA is the appropriate analysis to carry out if a given undesired event is defined and the goal is to determine its cause. Inductive approaches should be used if a given set of causes are identified and the goal is to determine the consequences. A comprehensive PRA might use both inductive and deductive
approaches to get a complete set of accident sequences depending on the complexity of the system.

### 2.4.2 PRA Extensions or Modifications

Yacoub and Ammar (2002), present a methodology for architecture-level risk analysis. Their approach is based on dynamic risk metrics (Yacoub, et al, 2000) that define complexity factors for architecture elements obtained from simulation of the software architecture specifications. FMEA is used with simulation to determine effects of a failure, and these results used to develop heuristic risk factors for all components and connectors. The risk factors are aggregated and used with component dependency graphs to analyze the overall risk for the architecture.

Wyss et al (2004) describe how features of event tree analysis and Monte-Carlo discrete event simulation can be combined with concepts of object-oriented analysis to form a new risk assessment technique (OBEST, object-based event scenario tree), though related to PRA. This OBEST method was developed to enable risk assessment study of systems and scenarios that exhibit strong time dependence, (not a characteristic of SCADA systems).

A natural extension to PRA involves the use of fuzzy concepts, though this approach has not been published for use in SCADA system security risk assessment. Early in the studies of risk analysis related to computer security, fuzzy modeling was used to analyze and rank risks in a computing facility. The authors created a set of fuzzy rules describing likely vulnerabilities such as “if the hard drive is old, then the customer database loss risk factor is increased”. These rules are combined to produce a total risk factor associated with the loss of the customer database. Similar rule sets and associated risk factors can be calculated for all computer facility assets. A similar procedure was used calculate a severity of loss for different components and then a total project risk in electronic commerce development.
Pillay and Wang, (2002) used fuzzy concepts to model the occurrence likelihood and consequences of failure for the identified hazards on a fishing vessel. They used FTA to calculate a “fuzzy” probability of the system failure. The consequences of failure for each basic event within the fault tree are considered for the four categories of negligible, marginal, critical, or catastrophic. The risk of the basic events is determined by combining the likelihood of occurrence and consequences of failure in linguistic terms via a fuzzy rule set. The output, once “defuzzified”, produces a risk ranking.

2.4.3 Attack Trees and Vulnerability Trees

Attack trees were introduced by Schneier (1999) as a way of formally analyzing the security of systems and subsystems based on varying attacks. This is basically FTA with the attack goal in place of a fault and basic event probabilities are not failure rates. Schneier’s work is notable because it was the first to apply this approach to the area of information security. The attack goal is the root of the tree and the different ways of accomplishing the attack are the leaves, with connections via AND and OR nodes.

Moore et al, (2001) describe and illustrate an approach for documenting attacks on software systems using attack tree information in a structured and reusable form. Analysts can then use the approach to document and identify commonly occurring attack patterns and then modify attack trees to enhance security development.

Most recently, attack trees have been applied to a SCADA communication system (Byres, et al, 2004). The authors identified eleven attacker goals and associated security vulnerabilities in the specifications and development of typical SCADA systems. They were then used to suggest best practices for SCADA operators and improvements to the MODBUS standard. Their application was qualitative in that attack tree analysis was used only to identify paths and qualify the
severity of impact, probability of detection, and level of difficulty. They did not calculate the probability of an actual attack being successful.

A related approach that arose in the computer and information security literature is vulnerability tree analysis. Vulnerability trees are hierarchy trees constructed as a result of the relationship between vulnerability and another vulnerability and or steps that a threat agent has to carry out to reach the top of the tree (Vidalis and Jones, 2003). Vulnerability trees help security analysts understand and analyze different attack scenarios that a threat agent might follow to exploit vulnerability. With this understanding, countermeasures can be taken.

2.5 Existing Risk Management Methodologies

Below will discuss about the existing methodologies of risk management. In this part SSE-CMM Model, COBIT Model, NIST Model, ISM3 Model, CRAMM Model and also SPMM Model will be described.

2.5.1 SSE-CMM Model

The International Systems Security Engineering Association (ISSEA, established in 1999) is a non-profit membership organization dedicated to the advancement of Systems Security Engineering as a defined and measurable discipline. The ISSEA has developed by an industry/government consortium a CMM, called the Systems Security Engineering Capability Maturity Model CMM (SSE-CMM). The SSE-CMM has been accepted by International Organization for Standardization (ISO) as ISO/IEC 21827 standard (ISSEA, Press Release). The SSE-
CMM model provides industry best practices guidance without being specific as to how security solutions are implemented, therefore, it can be used as a vehicle to generate security requirements. It is worth noting that the SSE-CMM adopts similar context of the Systems Engineering Capability Maturity Model (SE-CMM). The Table 2.1 and also the Figure 2.1 show SSE-CMM capability levels.

Table 2.1: SSE-CMM Capability Level (SSE-CMM Model Description Document, 2008)

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Base practices are performed informally</td>
</tr>
<tr>
<td>Level 2</td>
<td>Base practices are planned and tracked</td>
</tr>
<tr>
<td>Level 3</td>
<td>Base practices are well defined</td>
</tr>
<tr>
<td>Level 4</td>
<td>Base practices are quantitatively controlled</td>
</tr>
<tr>
<td>Level 5</td>
<td>Base practices are continuously improving</td>
</tr>
</tbody>
</table>
Figure 2.1: SSE-CMM Capability Levels (SSE-CMM Model Description Document, 2008)

Figure 2.2 and Figure 2.3 show the SSE-CMM appraisal process and SSE-CMM Capability Levels.
Figure 2.2: SSE-CMM Appraisal Process (SSE-CMM Appraisal Method (SSAM), 2008)

Figure 2.3: SSE-CMM Capability Levels (SSE-CMM Model Description Document, 2008)

The SSE-CMM defines eleven security-related Process Areas (PAs) and also includes another eleven process areas related to project and organizational practices (these process areas were adopted from the SE-CMM). Security-related process areas are defined in alphabetical order to avoid implications of a sequence (SSE-CMM):

PA01 – Administer Security Controls
PA02 – Assess Impact
PA03 – Assess Security Risk
PA04 – Assess Threat
PA05 – Assess Vulnerability
PA06 – Build Assurance Argument
PA07 – Coordinate Security
PA08 – Monitor Security Posture
PA09 – Provide Security Input
PA10 – Specify Security Needs
PA11 – Verify and Validate Security

Achieving capability level-1 on SSE-CMM requires 100% fulfillment of best practices predefined for this level. All other capability levels are considered achieved if 100% of the previous level and at least 80% of the current level is achieved.

SSE-CMM also identifies two types of metrics:

**Process Metrics:** Metrics that could be used as a measure of the level of maturity for a specific SSE-CMM process area. Hence, they tell whether or not a mature process exists.

**Security Metrics:** A measure of the efficiency for a particular SSE-CMM process area. They could be quantitative or qualitative measures.

The main difference between these two process metrics is that the first type offers information about the behavior of process areas, where the second type tests the output of these process areas.

### 2.5.2 COBIT Model

As part of COBIT® (Control OBjectives for Information and related Technology) initiative, the ITGI has developed a simple information security governance maturity model, which is meant to enable an organization to establish a ranking for the way it manages information security. COBIT maturity model is derived from the maturity model that the Software Engineering Institute defined for the maturity of software development capability. Figure 2.4 and Table 2.2 depicts various maturity states and generally describes requirements at each state respectively.
Figure 2.4 is about COBIT maturity model and Table 2.2 shows the levels of COBIT maturity model.

Figure 2.4: COBIT Maturity Model (COBIT Ver. 4, IT Governance Institute, 2008)

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 – Non-existent</td>
<td>The organization does not recognize the need for IT security. There is a complete lack of a recognizable system security administration process.</td>
</tr>
<tr>
<td>Level 1 – Initial / Ad hoc</td>
<td>The organization recognizes the need for IT security. But, the organization considers IT risks in an ad hoc manner, without following defined processes or policies.</td>
</tr>
<tr>
<td>Level 2 – Repeatable but intuitive</td>
<td>Responsibilities and accountabilities for IT security are assigned to an IT security coordinator. There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing.</td>
</tr>
<tr>
<td>Level 3 – Defined process</td>
<td>Security awareness exists and is promoted by management. An organization-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.</td>
</tr>
<tr>
<td>Level 4 – Managed and measurable</td>
<td>Responsibilities for IT security are clearly assigned, managed and enforced. The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management.</td>
</tr>
</tbody>
</table>
COBIT IT processes assume application controls are governed by business process owners and hence integrated into business processes, as a result, COBIT cover general IT controls. The maturity levels are meant to describe possible states of these IT processes. They are not intended for use as a fulfillment model, where fulfilling lower level requirements is an eligibility key to promotion to higher levels. For each of the predefined 34 IT processes, COBIT helps management to identify:

i. The actual performance of the enterprise: the current state
ii. The current status of the industry: for benchmarking purposes
iii. The enterprise’s target for improvement: the desired state

### 2.5.3 NIST Model

The Computer Security Resource Center (CSRC) under the National Institute of Standards and Technology (NIST) has developed a security maturity model based on five consecutive levels. The model links the maturity at any level with the level of documentation in place, and assumes fulfillment of previous level requirements in order to be promoted to higher level (i.e. NIST is a threshold model). Table 2.3 provides a brief description of the model details.

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Policies</td>
<td>Formal documented and updated policies are communicated to all employees. Policies establish a continuous risk assessment and implementation and cover major facilities and operations. Clearly assign roles, responsibilities, and measures.</td>
</tr>
<tr>
<td>Level 2: Procedures</td>
<td>Formal documented and updated policies cover all security controls. Procedures clearly identify where, how, when, and on what the procedure to be performed. Procedures document controls implementation.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Level 3: Implementation</td>
<td>Procedures are communicated to respective individuals and controls are implemented in consistent manner. Initial testing is performed.</td>
</tr>
<tr>
<td>Level 4: Test</td>
<td>Adequate tests are routinely performed to ensure that all policies, procedures, and controls are acting as intended. Effective corrective actions, self-assessments, and independent audits are performed.</td>
</tr>
<tr>
<td>Level 5: Integration</td>
<td>Policies, procedures, implementations, and tests are continually reviewed and improved. IT security program is embedded into culture and an integrated practice. Continuous cost-benefit analysis is performed.</td>
</tr>
</tbody>
</table>

### 2.5.4 ISM3 Model

Canal and his coauthors have developed a maturity model for Information Security Management (ISM). The model is called Information Security Management Maturity Model (ISM3 or ISM-cubed). This model is more abstract compared to other maturity models and is intended to evaluate and implement process-oriented information security management (ISM) systems. ISM3’s approach is based on the application of ISO9001 quality management concepts to ISM systems. ISM3 defines maturity in terms of the operation of key ISM processes and requires security to be aligned with business objectives. Processes are allocated to maturity levels according to a spectrum, from a basic ISM system to an advanced one with cost taken into account in order to realize return on investment at earlier maturity levels as shown in Figure 2.5.
The correlation between security improvement and investment on security is supported by Mayfield's Paradox:

*Keeping everyone out of an information system requires an infinite amount of money and getting everyone onto an information system requires an infinite amount of money, but the costs between these extremes are relatively low.*

An organization may choose to implement any of the defined processes at any stage of maturity assuming its relevance to specific security objectives. However, as clarified in Table 2.4, ISM3 defines five maturity models. Security risks and associated investment represent the sliding scale at every level in ISM3.

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISM3 Level 1</td>
<td>This level should result in a significant risk reduction from technical threats, for a minimum investment in essential ISM processes.</td>
</tr>
<tr>
<td>ISM3 Level 2</td>
<td>This level should result in further risk reduction from technical threats, for a moderate investment in ISM processes.</td>
</tr>
<tr>
<td>ISM3 Level 3</td>
<td>This level should result in the highest risk reduction from technical threats, for a significant investment in Information Security</td>
</tr>
</tbody>
</table>
ISM3 Level 4

This level should result in the highest risk reduction from technical and internal threats, for a high investment in Information Security processes.

ISM3 Level 5

This level assumes the compulsory use and continuous improvements of process metrics.

The deployment of ISM3 differs depending on whether or not there is an existing ISM system. If an ISM system is in place, the initiative starts by conducting a gap analysis of the systems and processes in place against the target ISM3 maturity level followed by ensuring that quality management is aligned with the organization’s security objectives and ISM3 standard. Otherwise (in case of new ISM implementation), the ISM3 is embedded into ISM formation process. However, Information Security Management consists of three management levels each of which has its own goals, practices, and processes:

i. Strategic (Direct and Provide), which deals with broad goals

ii. Tactical (Implement and Optimize), which deals with the design and implementation of the ISM system

iii. Operational (Execute and Report), which deals with achieving defined goals by means of technical processes

ISM3 is about process management. It suggests that, through well-defined processes, the information security is enhanced, risk is mitigated and, hence, maturity is measured. However, the performance of a well-designed ISM system depends on the budget, the capability and the commitment of those involved in running it. The use of ISM3 is about the way security is conducted. It does not guarantee that a process will perform properly or will deliver correct results, it only guarantees that the cause of faults is not ill-structured process.
2.5.5 CRAMM Model

The Central Computer and Telecommunications Agency (CCTA) was tasked by the UK Government's Cabinet Office to investigate the risk analysis and management methods currently in existence within Central Government for information security. As a result, a new framework was developed by CCTA which drew upon all of the existing best practices under the title of the CCTA Risk Analysis and Management Method (CRAMM). CRAMM is a comprehensive risk assessment tool that is compliant with BS7799 and ISO 17799. CRAMM has a database of over 3000 security controls referenced to relevant risks and ranked by effectiveness and cost. CRAMM addresses tasks such as:

i. Asset dependency modeling
ii. Business impact assessment
iii. Identifying and assessing threats and vulnerabilities
iv. Assessing levels of risk and identifying required controls

CRAMM implementation is a phased approach covering both technical and non-technical aspects of security. To evaluate these components, CRAMM is divided into three stages first is asset identification and valuation. The objective is to identify the physical, software, data and location of assets that make up the information system

Second stage is the threat and vulnerability assessment. The objective is to determine the likelihood of deliberate and accidental occurrences of various incidents and then to calculate the level of the underlying or actual risk

Third stage is countermeasure selection and recommendation. Utilizing the CRAMM countermeasure library (consists of over 3000 detailed countermeasures organized into over 70 logical groupings), appropriate countermeasures are selected
proportionately to predetermined assets and risk levels. CRAMM process will be show in Figure 2.6.

![CRAMM Process Diagram](image)

Figure 2.6: CRAMM Process (CRAMM, Version 5.1, 2008)

2.5.6 SPMM Model

The Security Program Maturity Model, developed by Chapin and Akridge, is an approach that distinguishes between maturity and quality of any security program and offers a model that measures both aspects and presents them combined together into one picture of security posture or dashboard display. Maturity from SPMM’s perspective is depicted by a simple judgment of the existence or nonexistence of large number of security elements derived from ISO17799 standard, where quality is depicted using a three-tiered quality factor: low, medium, and high, trying to transform the subjective metric (quality) into an objective one. Table 2.5 is about general outline of the security maturity model.
Table 2.5 SPMM: General outline of the security maturity model (Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005)
<table>
<thead>
<tr>
<th>ISO 17799 Categories</th>
<th>No. of Elements Measured</th>
<th>Items Covered by Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Overall security management</td>
<td>11</td>
<td>Business need, strategy, commitment, roles and responsibilities, policies and procedures</td>
</tr>
<tr>
<td>2. Asset classification and control</td>
<td>5</td>
<td>Valuation, risk assessment, business ownership, labeling and handling, inventory</td>
</tr>
<tr>
<td>3. Personnel security</td>
<td>8</td>
<td>Hiring and termination, roles and responsibilities, screening, training, reporting, review</td>
</tr>
<tr>
<td>4. Physical and environmental security</td>
<td>12</td>
<td>Perimeters, environmental hazards, risk assessment, access controls, safety, asset removal and destruction, monitoring, incident handling, awareness, cooperation</td>
</tr>
<tr>
<td>5. Access control</td>
<td>11</td>
<td>Perimeters, risk assessment, access controls, authentication, need to know, user responsibility, access updating, monitoring, mobile computing, incident handling</td>
</tr>
<tr>
<td>6. System development and maintenance</td>
<td>9</td>
<td>Standards, life cycle model, review, gap analysis, requirements planning, testing integrity and certification, code repository, release management, retirement</td>
</tr>
<tr>
<td>7. Communications and operations management</td>
<td>16</td>
<td>Standards, all methods of e-communications, operations procedures, monitoring, backups, exception handling, updates and patches, help desk, change management, cryptographic systems, media handling, malicious code, system acceptance, documentation library, capacity planning</td>
</tr>
<tr>
<td>8. Organizational security</td>
<td>11</td>
<td>Security function, monitoring, advisory, auditing, forum, awareness training, segregation of duties, penetration and vulnerability testing, incident handling, cooperation</td>
</tr>
<tr>
<td>9. Business continuity management</td>
<td>7</td>
<td>Risk assessment, prioritization, backups, business continuity/ disaster recovery planning, testing, updates</td>
</tr>
<tr>
<td>10. Compliance</td>
<td>10</td>
<td>Regulatory, contractual, intellectual property, labeling and handling, record retention, auditing, sanctions</td>
</tr>
</tbody>
</table>

Table 2.5 describes the ISO17799 domains covered by the model and associated elements of each.

Table 2.6 is about sample elements from security maturity model.
Table 2.6: SPMM: Sample elements from security maturity model (Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005)

<table>
<thead>
<tr>
<th>Order Performed</th>
<th>Program Maturity Elements—2. Asset Classification and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.1 Valuation is performed to identify and understand information assets to protect.</td>
</tr>
<tr>
<td>2</td>
<td>2.2 Risk assessment is performed to identify and quantify threats to information assets.</td>
</tr>
<tr>
<td>3</td>
<td>2.3 Information assets have defined system custodians and business owners.</td>
</tr>
<tr>
<td>4</td>
<td>2.4 Information assets classification labeling and handling procedures are developed.</td>
</tr>
<tr>
<td>5</td>
<td>2.5 An asset management inventory program is installed to handle assets on an ongoing basis.</td>
</tr>
</tbody>
</table>

Table 2.6 clarifies the maturity using a sample of one domain (Asset Classification and Control) and the model suggested order for the implementation of its elements.

The following is table 2.7 and about Sample of a quality measure from security maturity model:

Table 2.7: SPMM: Sample of a quality measure from security maturity model (Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005)

<table>
<thead>
<tr>
<th>Program Maturity Element</th>
<th>If maturity element is implemented, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low-quality Threshold</td>
</tr>
<tr>
<td>2.4 Information Assets classification labeling and handling procedures developed</td>
<td>Procedures developed but not implemented</td>
</tr>
</tbody>
</table>

Table 2.7 depicts the quality of a specific element as a successor step of its maturity.

2.6 OCTAVE Model

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) is a risk-based strategic assessment and planning technique for
security developed at Carnegie Mellon University. The OCTAVE approach considers both organizational and technological issues. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization’s security strategy.

![OCTAVE Process Diagram](image)

Figure 2.7: OCTAVE Process (Introduction to OCTAVE approach, Carnegie Mellon, Software Engineering Institute August 2003)

Three main things in the OCTAVE process is Build Asset-Based Threat Profiles, Identify Infrastructure and also Develop Security Strategy and Plans Vulnerabilities. These three process will determine the strategy for the organization to help in reduce the risk of organization.

2.6.1 Three Aspects – Three Phases

The organizational, technological, and analysis aspects of an information security risk evaluation lend it to a three-phased approach. OCTAVE is organized around these basic aspects (illustrated in Figure 2), enabling organizational personnel
to assemble a comprehensive picture of the organization’s information security needs. In Section 6 of this document, we explore the phases of OCTAVE in greater detail. The phases are:

**Phase 1: Build Asset-Based Threat Profiles** – This is an organizational evaluation. Staff members from the organization contribute their perspectives on what is important to the organization (information-related assets) and what is currently being done to protect those assets. The analysis team consolidates the information and selects the assets that are most important to the organization (critical assets). The team then describes security requirements for the critical assets and identifies threats to the critical assets, creating threat profiles.

**Phase 2: Identify Infrastructure Vulnerabilities** – This is an evaluation of the information infrastructure. The analysis team identifies key information technology systems and components that are related to each critical asset. The team then examines the key components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets.

**Phase 3: Develop Security Strategy and Plans** – During this part of the evaluation, the analysis team identifies risks to the organization’s critical assets and decides what to do about them. The team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.

### 2.6.2 Principles of OCTAVE

Principles are the fundamental concepts that define the philosophy behind the evaluation process. They shape the evaluation approach and provide the basis for the evaluation process. We have grouped the principles into the following three areas:
• **Information Security Risk Evaluation Principles**: These are key aspects that form the foundation of effective information security risk evaluations.
  
  – self direction
  – adaptable measures
  – defined process
  – foundation for a continuous process

• **Risk Management Principles**: These are basic principles common to effective risk management practices.
  
  – forward-looking view
  – focus on the critical few
  – integrated management

• **Organizational and Cultural Principles**: These are aspects of the organization and its culture that are essential to the successful management of information security risks.
  
  – open communication
  – global perspective
  – teamwork

Figure 2.8 shows three principles of the OCTAVE. First is organization and cultural principle, risk management principle, information security risk evaluation principle.
Figure 2.8: Principles of OCTAVE (OCTAVESM Criteria, Version 2.0 Christopher J. Alberts Audrey J. Dorofee, 12-2001)
CHAPTER 3

METHODOLOGY

3.1 Introduction

To develop any system, choosing a suitable methodology is important to ensure the quality of system. Therefore, this chapter will include some studies of methodology that need to apply to this system development. The chosen methodology will be the guild to help to complete the system. Besides, this chapter will also include the system requirements analysis for hardware and also software.

3.2 Project Methodology

Prototyping methodology is the selected tool to help to develop system. Typically, users know many of the objectives that they wish to address with a
system, but they do not know all the nuances of the data, nor do they know the
details of the system features and capabilities. The Prototyping Model allows for
these conditions, and offers a development approach that yields results without
first requiring all information up-front. When using the Prototyping model, the
developer builds a simplified version of the proposed system and presents it to
the customer for consideration as part of the development process. The customer
in turn provides feedback to the developer, who goes back to refine the system
requirements to incorporate the additional information. Often, the prototype
code is thrown away and entirely new programs are developed once
requirements are identified. This is the process flow for the prototyping model

Figure 3.1: Process Flow of an application Design in Evolutionary Prototyping.
1.1 Planning Phase

Planning phase is the first phase of this process flow. This phase is to identify the general objective, scope of project, users of that are involve in this project. The activity for this phase includes time scheduling and assigns each task with specified time frame. Microsoft Project 2003 software will be use to create a Gantt chart where it will list all the activities and the estimated time frame. Gantt chart just acts as a reminder and assumption for the project.

1.2 Analysis Phase

All the literature review that has been done is to help create more understanding to developing knowledge useful to this project. In this phase, the research and study that had been done need to be use to create an effective system. By compare with existing system, this will improve my project become effective and efficient usability of a software system.

1.3 Design Phase

In this phase, the main activity is to design the database and define the specification requirements of system input and output In this system design, class
object and data field that involve will be create into use-case diagram, sequence diagram also class diagram by using UML and Rational Rose.

1.4 Development Phase

In this phase, process programming and coding will be done. And the coding will process by using some software. The executable application will also be done in this phase and the prototype model will be tested to reach the specific requirement and also to satisfy the needs of user. If there is some unsatisfied or maybe requirement does not met then the prototype will be modify until all is accepted then only can proceed it to the next phase.

1.5 Implementation and Evaluation Phase

This is the last phase of the process. In this phase, the complete prototype will be tested to satisfied the user requirement if the prototype is not accepted then some modification will be done until the prototype is passed. When the evaluation process has passed, the prototype is considered a final product and can begin implementing into reality.

3.2.6 Advantages of Prototyping:

i. Users are actively involved in the development
ii. It provides a better system to users, as users have natural tendency to change their mind in specifying requirements and this method of developing systems supports this user tendency.

iii. Since in this methodology a working model of the system is provided, the users get a better understanding of the system being developed.

iv. Errors can be detected much earlier as the system is mode side by side.

v. Quicker user feedback is available leading to better solutions.

3.2.7 **Disadvantages of Prototyping:**

i. Often clients expect that a few minor changes to the prototype will more than suffice their needs. They fail to realise that no consideration was given to the overall quality of the software in the rush to develop the prototype.

ii. The developers may lose focus on the real purpose of the prototype and compromise the quality of the product. For example, they may employ some of the inefficient algorithms or inappropriate programming languages used in developing the prototype. This mainly due to laziness and an over reliance on familiarity with seemingly easier methods.

iii. A prototype will hardly be acceptable in court in the event that the client does not agree that the developer has discharged his/her obligations. For this reason using the prototype as the software specification is normally reserved for software development within an organisation.

3.3 **System requirements analysis**
In order to make sure the development of system can proceed with systematically and smoothly, some hardware and software requirements are need to be defines. There are two groups of people that are developer and the system user. In the justification of hardware will focus on both groups. But the software requirements only focus for developer.

3.3.1 Hardware Requirements

Suitable hardware will ensure the system can operating smooth and completely. Developer and system user they got different requirement for the system. Developer need more high speed processor to run the software and more high RAM to make sure can open multi software at one time. But for the system user they just need very low processor and also very low RAM support this system.

3.3.1.1 Hardware Requirements for Development

The hardware that is used to develop this system is:

i. Intel Pentium IV 1.5GHz Processor and above
ii. 512 MB DDR2 RAM and above
iii. 20 GB of hard disk free space

3.3.1.2 Hardware Requirements for System User
To run this system the user need:

i. Intel Pentium III 0.3 GHz Processor and above
ii. 128 MB DDR2 RAM and above
iii. 20 GB of hard disk free space

3.3.2 Software Requirements.

Software requirement for develop this system is operating system (Window XP), MySQL, WampServer, Macromedia dreamweaver, Firefox internet explorer, Rational rose 2000, Microsoft access.

3.4 Summary

For develop a system, methodology is important to make the system more systematic and tidy. In this chapter, phases of the methodology will be discussed and this will help in achieve system objective and fulfill the need of the system.
CHAPTER 4

SYSTEM DESIGN

4.1 Introduction

This chapter will do all the activity of design phase. Activity like system architectural design, use-case diagram, sequence diagram and the user interface design need to be prepared in this chapter as well. All the design and diagram will be use as a references when start to develop the system. Besides, the system design may help to determine the system whether it is satisfied the client needs or not.

4.2 System Architectural Design
For this architectural design include staff, computer, and database. Staff inside this architectural design is to contribute the information of the organization and also their own knowledge about the job. After all the inputs are filled in then the user can save the data or information inside database then they can choose to print out the a report of that or just exit. Figure 4.1 below is the system architectural design.

![Figure 4.1: System Architectural Design](image)

**4.3 System Analysis**

In this phase, *Unified Modeling Language* (UML) has been used to model and develop the needs of this system. By using this language, use-case diagram will be used to show the functionalities of the system. Besides, all the functions will be described in this section also.
4.3.1 Use-case Diagram

This system consists of two actors and they are admin and analyzer. Following is description for the task of actors inside this system.

Figure below is figure 4.2 and figure 4.3. figure 4.2 is about function that can use by admin and figure 4.3 is the function that can use by user

![Use-case Diagram](image)

Figure 4.2: Use case diagram for admin i. Admin

This actor is to control the database and the system. Admin will change the database if there is an update or some changes needs to be done. Admin will ensure the output from database is updated. Admin also can insert update or delete user.
User only need to store required information to system then stores it into database. They can choose to print out the report or just exit this system. They need to choose which phases of information they want to fill.

### 4.3.1.1 Description of use case

Basically, admin will use the system only when there is some update or error for the database. They can set the users who want to use this system. Admin can delete the user and also can add a user into the system so that they can start to use it.

User need to fill the information according the needs of the OCTAVE. User need to fill the asset, vulnerability, threads of the organization. So they need to understand the operation of organization very well. After filled in the information user

### 4.4 Sequence Diagram
The following Figure 4.4 shows that the process of admin to delete data from database. When admin want to delete an id of a user so they can use the delete function.

Figure 4.4: Sequence diagram for delete data
Below is Figure 4.5, and it shows how to update data by admin of this system. Admin will do this maybe when a user needs to change password or some attribute need to change.

Figure 4.5: Sequence diagram for update data

Figure 4.6 shows the way of insert a new data into database. When got new staff or new user for the system admin may insert the new user for this system so that the user can start to use this system
There are three activities for user to do in this system. First is build enterprise-wide security requirements and second is identify infrastructure vulnerabilities and lastly is determine security risk management strategy. These three activities using the same way when operation. User can print the report when they fill in the fields. At the same time they can choose exit that system or proceed to the next phases also. The sequence diagram in Figure 4.7 shows the way how the system runs.
4.5 Database Design

10 tables was created in the database and named as db_octave. For this system database is use to store the user input of the worksheets. The input will be process and take out from database when user wants to view the report. Figure 4.8, Figure 4.9 and also Figure 4.10 are the database of the system.
Figure 4.8 Database of registered user

Figure 4.8 shown the database of registered user and this database stored username, password, position of the worker, and also usertype. Usertype in this database is to determine the type of user.

Figure 4.9 Database of Asset Group Worksheet

Figure 4.9 is the database that is store data of asset group worksheet and it will store asset, importance of asset, and also the user that filled in the data into the database.
Figure 4.10 Database of Questionnaire

| Q1   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q2   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q3   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q4   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q5   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q6   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q7   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q8   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q9   | varchar(20) | latin1_swedish_ci | No | | | | |
| Q10  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q11  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q12  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q13  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q14  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q15  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q16  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q17  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q18  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q19  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q20  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q21  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q22  | varchar(20) | latin1_swedish_ci | No | | | | |
| Q23  | varchar(20) | latin1_swedish_ci | No | | | | |
| username | varchar(255) | latin1_swedish_ci | No | | | | |
| position  | varchar(255) | latin1_swedish_ci | No | | | | |

Figure 4.10 show the database of questionnaire, answers of the data of this table are “YES”, “NO” and “Don’t Know”. When user store the answer into database their name and position will be recorded also. This is because when next time the same user login they can continue to do the incomplete survey or update new answer for this survey.

4.6 Interface Design

System interface design is one of the important parts of a system. The interface shows the user-friendly function and hides the complicated data. Users will
interact with the system and they need an easy understand interface so that they can manipulate it well.

Figure 4.11: Interface design for the worksheets.

On the figure 4.8 above shows the interface design for the worksheets and basically all worksheets page design are the same just the content of worksheets are different only.

Figure 4.12: Interface design for the login page
Figure 4.9 shows the login page of this octave system. This page will lead the user to the worksheets that they need to fill in by indentified the position of the user.

![octave system](image)

Figure 4.13: Interface of Log out page

Figure 4.10 just inform the user that they already logged out from the system. User can choose to login again to the page or direct leave this system. Even they logged out users still can view the report of the research.

4.7 Summary

In this chapter, lots of interfaces will be presented for example database interface, design interface, use-case diagram, and also sequence diagram.
Chapter 5

IMPLEMENTATION

5.1 Introduction

This chapter is more focus about the coding part of the system and implementation of the system will be discussed in this chapter too. Development software is important to make sure this system can run and process smoothly and the system testing also will be done. From doing system testing bugs will be found out so that the debug will only be done.

5.2 Development Environment

This part is about development environment and there is some software that is uses when develop the system.
5.2.1 Installation of Required Software

Software that needs to be installed: Macromedia Dreamweaver 8, WampServer, Rational Rose 2005, and Microsoft Project 2003.

Macromedia Dreamweaver is the main software on design this Octave system. This system is a web-based system and macromedia provide more convenient function for user to done their system. Server will be needed for this system. WampServer is to creating database.

For architecture design part, Rational Rose 2005 is needed to design the use-case, class diagrams. Finally the Microsoft Project 2003 is used to do planning and generate Gantt chart for this project.

5.3 Coding

All the coding of the system is presented in this part. Database connect coding, login coding and also coding about insertion of data into database.

5.3.1 Database connect

Figure 5.1 shows how the database connection to mysql server and also show the database selecting.
<?php

// login to MySQL Server from PHP
$conn = mysql_connect("localhost","root","");

// If login failed, terminate the page (using function 'die')
if (!$conn) die("Error when connecting to MySQL: ". mysql_error() );

// Login was successful. Then choose a database to work with
$selected = mysql_select_db("db_octave",$conn);

// If required database cannot be used, terminate the page
if (!$selected) die ("Cannot use database: ". mysql_error() );
?

Figure 5.1: Database Connection

5.3.2 Login coding

Figure below shows the login code for Octave system. Inside figure 5.2 is the php code that read variables from previous page then compare the username and password. After make sure the username and password are correct then the coding will redirect the page by indentify the user type.
<?php
session_start();
include "dbconn.php";

$username = $_POST['username_login'];
$password = $_POST['password_login'];
if($username==""&&$password=="")
{
    header("Location:".$_SERVER['HTTP_REFERER']);
    exit;
}
$sql = "SELECT * FROM user WHERE username = '$username' AND password = '$password'";
$result = mysql_query($sql) or die('Query failed. '.mysql_error());
$usertype=0;
if (mysql_num_rows($result) == 1)
{
    $row = mysql_fetch_row($result);
    $position = $row[2];
    $usertype
    if($usertype==1)
    {
        $_SESSION['userposition']=$usertype;
        $_SESSION['username']=$row[0];
        header('Location:admin.php');
        exit;
    }
    else if($usertype==2)
    {
        $_SESSION['userposition']=$position;
        $_SESSION['username']=$row[0];
        header('Location:process1.php');
        exit;
    }
    else if($usertype==3)
    {
        $_SESSION['userposition']=$position;
        $_SESSION['username']=$row[0];
        header('Location:process2.php');
        exit;
    }
    else if($usertype==4)
    {
        $_SESSION['userposition']=$usertype;
        $_SESSION['username']=$row[1];
        header('Location:process3.php');
        exit;
    }
}
if (mysql_num_rows($result) != 1)
{
    header('Location:login_error.php');
    exit;
}
?>

Figure 5.2: Login

5.3.3 Insert of data
In figure 5.3 below is one of the data insert. In this system there is a lots of data insert and only one of them will be show and the rest will be mostly then same. The frequent of the data insert will be start from connecting database then define the query for insertion then redirect to another page.

```php
<?php
session_start();
eextract($_POST);
include "dbconn.php";

$query = mysql_query("insert into smk VALUES (" , " , " , 'Textfield', 'Textfield2' , " , " , ");
if(!$query) die("SQL query error encountered : ".mysql_error());

header('Location:http://localhost/psm%20website/process1b.php');
exit;
?>
```

Figure 5.3: Insert of data

5.4 Conclusion

As a conclusion, this chapter discussed about the implementation of the system and this may help to improve the stability of the system and its consistency.
CHAPTER 6

DISCUSSION AND CONCLUSION

6.1 Introduction

Achievement, challenges and also expectation are discussed in this chapter. Risk management is important for every organization and it can prevent an organization from loss. So this Octave is one of the risk management tools to help to decrease the risk of an organization. This system makes users more convenient on keeping the worksheets that had been done in database but no anymore in file. Beside the lots of paper work would not be needed anymore because all can be done by using this system.

6.2 Achievement

Firstly, I have understood about my project. This includes the objectives, scopes, importance of the project. These entire things I had done in chapter 1. Secondly, in literature reviews I have some research on the similar existing system to
help in my development. Besides, I also have a deeper understanding about my project. By doing this I can more clear about my project and the weakness or strength when compare to other existing methodologies. Next, a suitable methodology is important when creating a system. So need do some research on choosing methodology. After research, prototyping is the chosen methodology for me to develop my system. Furthermore, in the previous chapter which was included the system design, use-case diagram, sequence diagram, database design and also the interface design. Even thought that jus a roughly design and this may help me proceed and develop my system smooth and faster. Lastly, implementation part and system testing helps in find bugs and make the system can run smoothly and prevents any unwanted error occur.

6.3 Challenges

Many time spent to understand the topic. Beside this, OCTAVE is a document form and there is no existing software available for now. To convert these manual sheets to system is taking lots of time. In the report generation part, the format of the report is hard to set and there is no standard format to follow.

6.4 Expectation

This system is created for organizations to help them manage their risk problems and also in handling threads, but some others aspect also can be improve to help to maximize the quality of this system. Here is some expectation that can help to make the system better:
i) Interface design can be make by flash that will be more attractive and also more user-friendly.

ii) Security of the system can be change to more secure for example like encrypt the password.

iii) Convert into an intelligent system that can auto generates the strategy for organization.

6.5 Summary

This project is a web-based system that converts the complicated worksheets into simple web form that can help organization to keep the data or information on software. So because of this, Octave system will bring benefits to the organization. This system is developed by using php programming language, and some software like Macromedia Dreamweaver, MySQL to make the system can function well. Manual worksheets will be no longer needed and this can prevent the losing of the data the already filled inside the worksheets. System fulfill the objectives, scope that already stated in the early of the report.
REFERENCES


and Survivability,” Technical Note, CMU/SEI-2001-TN-001, Software Engineering
Institute, Carnegie Mellon University.

Vulnerabilities in SCADA Systems,” International Infrastructure Survivability
Workshop (IISW’04), IEEE, 9.

Threat Assessment, Available at
Appendix A
GANTT CHART
Appendix B
User Manual
Login Page

This is the main page that is let user to login. There are two fields in this page user require to fill in their registered account username and password to start the form. User also can view the report of analysis over here.

Login Error Page
After checking the password, the system will show this page if the system detects that the password is incorrect and there is a link for the user to log in again.

**Admin Page**

![Admin Page Diagram](image-url)

**Figure C3: admin page**
After login and the system will process the password and check the usertype of the user to open the website. Add button is for admin to enroll new user to this system. After fill in those fields and press “add” then new users will be enroll in the system.

Analysis Form

Figure C4: Analysis form page

After login for normal staff this analysis form will appears in window and user needs to fill in the fields. And summit button is for user store the input into database. If the user let it blank and he can update it when he is free.
Area Of Concern Worksheet

After user fill in the number of fields and press “create” button below there will appear the fields.

Figure C5: Area of concern worksheet
Survey Form

Figure C6: Survey Form

This is the survey form for user to fill in. After press summit button the data will store into database.
This page will introduce the OCTAVE method. User can edit the data that are already or no yet fill in. User also can choose to leave this system by press the logout button.
Report Link

![Image of report link](image)

Figure C8: Report Link

There are some links that can let user to open the report of the risk analysis.
Report Interface

![Report Interface Diagram](image)

**Figure C9: Report Interface**
This is the sample of the report that generated after user fill in the form.

Logout Interface

![Logout Interface](image)

Figure C10: Logout Interface

System will thank the user when user logout from this system. User can choose login again or quit this browser.