UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : **MOHD NAZER BIN APAU**

Date of birth : **27th FEBRUARY 1976**

Title : **THE ANALYSIS AND DEVELOPMENT OF SECURE SOFTWARE ASSESSMENT MODEL (SSAM) CASE STUDY: ONE OF THE MAJOR FINANCIAL INSTITUTION**

Academic Session: **2007/2008**

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 ACCESS**	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.
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.

Certified by:

SIGNATURE	**SIGNATURE OF SUPERVISOR**
760227-04-5193	**RABIAH AHMAD**
(NEW IC NO. /PASSPORT NO.)	**NAME OF SUPERVISOR**
Date :	Date :

NOTES : * If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

20 November 2007

Librarian
Perpustakaan Sultanah Zanariah
UTM, Skudai
Johor.

Sir,

CLASSIFICATION OF THESIS AS RESTRICTED - THE ANALYSIS AND DEVELOPMENT OF SECURE SOFTWARE ASSESSMENT MODEL (SSAM) CASE STUDY: ONE OF THE MAJOR FINANCIAL INSTITUTIONS BY MOHD NAZER BIN APAU

Please be informed that the above mentioned thesis entitled "The Analysis and Development of Secure Software Assessment Model (SSAM) Case Study: One of the Major Financial Institutions" be classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are:-

(i) Thesis contains some confidential information regarding the case study organization's process flow and standard operating procedure, and
(ii) The contents display some information about the bank's participated vendors

Thank you.

Sincerely yours,

……..

Dr. Rabiah Ahmad
rabiah@citycampus.utm.my
J2803 – Fakulti Sains Komputer dan Sistem Maklumat (CASE)
03-26154756

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Information Security"

Signature : .....

Name of Supervisor I : .....

Date : .....

Signature : .....

THE ANALYSIS AND DEVELOPMENT OF SECURE SOFTWARE ASSESSMENT MODEL (SSAM) CASE STUDY: ONE OF THE MAJOR FINANCIAL INSTITUTIONS

MOHD NAZER BIN APAU

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

Faculty of Computer Science and Information Systems
University Teknologi Malaysia

NOVEMBER 2007

I declare that this thesis entitled "*The Analysis and Development of Secure Software Assessment Model (SSAM) Case Study: One of the Major Financial Institution*s (Malaysia)" 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 : **Mohd Nazer bin Apau**

Date : …….....

To my wife Izam Zuliana Yahya, and
children Zarif Aiman , and Nur Zara Safiah
Also to my beloved mother and father for their patience, understanding, and dedication

ACKNOWLEDGEMENT

IN THE NAME OF ALLAH, MOST GRACIOUS, MOST COMPASSIONATE

Thank you to Allah for giving me the blessing for health, strength and earnestness to accomplish and fulfill my final project report. I take this opportunity to convey my utmost gratitude and appreciation to my supervisor, Dr. Rabiah Ahmad and Pn. Salmah Awang who gives me the full support and all guidance, advice and commitment upon my effort to complete this report.

This appreciation also goes to my beloved family, lecturers and friends who always encourage and give me full support when needed. Indeed, the courage and support is highly appreciated.

ABSTRACT

Software evaluation can sometime become a problem in determining on how extensive to which a software products satisfies a set of requirements. Decision in choosing the right solution is a challenge to every organization. Conceptually, there is no right or wrong procedure in dealing with software purchases; however a consistent and transparent approach within the evaluation committee is important to ensure a high quality gathered from the end product. As for a big organization, choosing the right solution from the right vendors is crucial in order to ensure the business objective and goals are not interrupted. The problem with the situation is always on resources in term of people, process and skills with regards to the technology acquired. Insufficient number of people may contribute to the lack of quality output in finding out the best solution. Lack of skills in term of the requirement and technical "know-how" and "know-who" in choosing the right vendors may as well contribute to non-conformance product. The improper process of finding the solution is also can lead to the above problem. All mentioned problems can be aggregate with more shortcomings i.e. to incur more effort and cost to the organization in rectifying the problem. Introducing Secure Software Assessment Model (SSAM) can assist the organization to have a proper evaluation process with regards to security properties. Indirectly, implementing SSAM can also create more awareness on security requirements among users and solution providers. It would then reduce the problem facing by the organization in term of lacking compliances to the IT Security Policy.

ABSTRAK

Menilai perisian komputer atau produk boleh menimbulkan masalah kepada mana-mana organisasi dalam menentukan betapa spesifikasi produk terhadap keinginan organisasi dapat dipatuhi. Membuat keputusan untuk mana-mana perisian yang sesuai merupakan aspek yang mencabar bagi mana-mana organisasi. Secara mana sekali pun, memang tidak ada jalan yang mudah mahupun jalan yang betul atau yang salah dalam menentukan perisian yang sesuai di sesebuah organisasi. Tetapi kaedah yang teratur, konsisten dan telus di dalam pasukan penilaian adalah penting bagi memastikan apa yang dipilih berkualiti tinggi. Bagi syarikat-syarikat besar, penilaian ini adalah penting untuk memastikan tidak ada gangguan operasi kelak. Masalah-masalah ini timbul selalunya berdasarkan manusia, proses dan kemahiran terhadap sesuatu teknologi. Kurangnya tenaga kerja boleh mendatangkan kemudaratan terhadap kualiti pengeluaran. Kemahiran yang kurang terhadap teknikal dalam memilih resolusi juga boleh menjejaskan hasil kerja dan menyebabkan perisian yang diperolehi tidak mencapai tahap piawaian yang dingini. Proses yang tidak tepat juga boleh menyebabkan apa yang dibincangkan tadi boleh berlaku. Kesemua ini boleh berlaku dan menjejaskan apa yang ingin dicapai oleh sesebual organisasi. Dengan memperkenalkan Penilaian Perisian Berdasarkan Keselamatan Maklumat atau "*Secure Software Assessment Model (SSAM)*", ia dapat membantu organisasi dengan cara pengendalian penilaian yang betul mengenai keselamatan maklumat perisian. Ini juga membantu organisasi dengan kesedaran yang lebih mendalam kepada aspek keselamatan maklumat dikalangan pengguna dan pembekal perisian. Masalah yang dihadapi oleh organisasi dalam kurangnya tahap piawaian terhadap polisi keselamatan maklumat juga dapat dibendung.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xii
	LIST OF APPENDICES	xiii
1	**INTRODUCTION**	
	1.1 Overview	1
	1.2 Background of Selected Study Organization	1
	1.3 The Background of Problem	4
	1.3.1 Lack of Compliances to IS Security Policy	5
	1.3.2 Staff Constraint	6
	1.3.3 Cost	6
	1.4 The Objective	7
	1.5 Scope	8
	1.6 Project Importance	10
	1.7 Project Plan	11
	1.8 Summary	12

2	**LITERATURE REVIEW**		
	2.1	Introduction	13
	2.2	Techniques and Approach	14
	2.3	Common Criteria	16
	2.4	Architecture Trade-off Analysis Method	18
	2.5	Qualitative Selection	20
	2.6	SDLC Phase 0: Evaluation	26
		2.6.1 Introduction	26
		2.6.2 Initiations and Endorsement	27
		2.6.3 Source for Solution	28
		2.6.4 Assessment and Selection	29
		2.6.4.1 Functional and Technical Review	29
		2.6.4.2 Cost Implication Review	31
		2.6.4.3 Overall Assessment	31
		2.6.4.4 Recommendation	32
	2.7	Commercial of the Shelf (COTS) Evaluation	3
		2.7.1 Plan the evaluation	34
		2.7.2 Design the evaluation instrument	34
		2.7.3 Apply the evaluation instrument	34
	2.8	Summary	35
3	**PROJECT METHODOLOGY**		
	3.1	Introduction	36
	3.2	Operational Framework	36
		3.2.1 Data Collection and Analysis	37
		3.2.2 Pilot Study	38
		3.2.3 Evaluate the Result	38
		3.2.4 Develop Prototype	38
	3.3	Summary	39

4	**ANALYSIS AND DESIGN**		
	4.1	Introduction	40
	4.2	Secure Software Assessment	40
	4.3	Mapping on Activity between SDLC Phase 0 and COTS Model	43
	4.4	Generic Secure Software Assessment model	45
	4.5	IT Security Baseline Requirement	46
		4.5.1 Physical Security	47
		4.5.2 Network Security	47
		4.5.3 Application Security	48
		4.5.4 Database Security	48
		4.5.5 System Security	49
		4.5.6 ID Security	49
		4.5.7 Operational Management	49
		4.5.8 Logical Security	50
		4.5.9 Policies	50
	4.6	Summary	51
5	**RESULT AND DISCUSSION**		
	5.1	The Result of SSAM Implementation	52
	5.2	The Result of Pilot Project Implementation	53
	5.3	Summary	58
6	**CONCLUSION**		
	6.1	Conclusion	59
	6.2	Summary of Contribution	61
REFERENCES			62

LIST OF TABLES

TABLE NO	TITLE	PAGE
1.1	SDLC Phases	2
1.2	IS Security Policies	9
2.3	Scoring Table	21
2.4	Vendor Self-Evaluation scale	23
2.5	Risk Factor	24
2.6	Vendor Self-Evaluation Score scale	24
2.7	SDLC Phase 0: Fix Scoring for Functional and Technical	29
4.8	COTS and SDLC Phase 0	42
4.9	IT Security Baseline Requirement Section	44
5.10	Project 1 for Vendor A	52
5.11	Project 1 for Vendor B	53
5.12	Project 2 for Vendor A	54
5.13	Project 2 for Vendor B	54
5.14	Project 2 for Vendor C	55

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
1.1	Project Life Cycle	3
1.2	Project Activities	11
2.3	Security Software Assessment and SDLC Phase 0	26
3.4	Operational Framework	35
4.5	COTS and SDLC Phase 0	42
4.6	Secure Software Assessment Model	44
5.7	Vendor Compliances Chart	57

LIST OF ABBREVIATIONS

GITSC	–	Group IT Steering Committee
LTM	–	Logical Technology Model
ORM	–	Operational Risk Management
PTM	–	Physical Technology Model
RD	–	Requirement Definition
WO	–	Work Order
COTS	–	Commercial of the Shelf
RFI	–	Request for Information
RFP	–	Request for Proposal
Org.	–	Organization
R&R	–	Roles and responsibilities
ITSEC	–	IT Security
BAFO	–	Best and Final Offer
CMM	–	Capability Maturity Model

LIST OF APPENDIXES

APPENDIXES	TITLE	PAGE
A	IT Security Baseline Requirements	64
B	IT Security Baseline Compliance Table	103
C	IT Security Baseline Prototype Scoring Calculation	105

CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter begins with the background of the selected case study organization. In section 1.2 it briefly explains on the current process in dealing with a software development and a project life cycle. One of the focus areas is software evaluation. Section 1.3 highlights the difficulty face by the organization if the proposed Secure Software Assessment Model (SSAM) is not in place. Chapter 1 emphasizes on the objective of having SSAM with explaining on the scope and the importance of SSAM.

1.2 Background of the Selected Study Organization

The organization selected for the case study is well known as the largest banking group in Malaysia. It has been the leading for the banking industry with over three and a half decades. This organization has established around 500 branches nationwide and available in most of the major cities globally. In order to better manage and concentrate the core businesses, the organization has outsourced the IT infrastructure related matters to the United States fortune 500 companies. Currently, the organization has about 500 staffs in IS Sector to support the organization in IT operation for growth and innovation.

Within the outsource environment, the process of implementing IT project is very crucial. It is a known fact that each IT project implementation involves a new software deployment. Staff within the organization is expected to comply with the System Development Life Cycle (SDLC) framework where it consists of Phase 0 until Phase 9 as illustrated in Table 1.1 below. The organization's Project Life Cycle (PLC) framework has two main processes which are SDLC and Account Project Management Office (APMO). SDLC is used to govern the software development life cycle while APMO is governing the infrastructure related matters. This is consisting of network operation setup, server preparation, server hardening and the port scanning activities. Figure 1.1 representing the organization high level process of SDLC and APMO.

System Development Life Cycle (SDLC) – Phase 0 to 9	
Phase 0	Evaluation – software initiation or product evaluation
Phase 1	System Analysis and Design – product initiation
Phase 2	Functional Specification – documenting functional requirements
Phase 3	Technical Specification – documenting technical requirements
Phase 4	Installation – product or software installation for development and testing
Phase 5	Programming – product development
Phase 6	Testing – verification on technical and functional requirements
Phase 7	Documentation – compiling all project evidence
Phase 8	Implementation - product or system cut over / live
Phase 9	Post Implementation Review (PIR) – review product / lesson learnt

Table 1.1: SDLC Phases

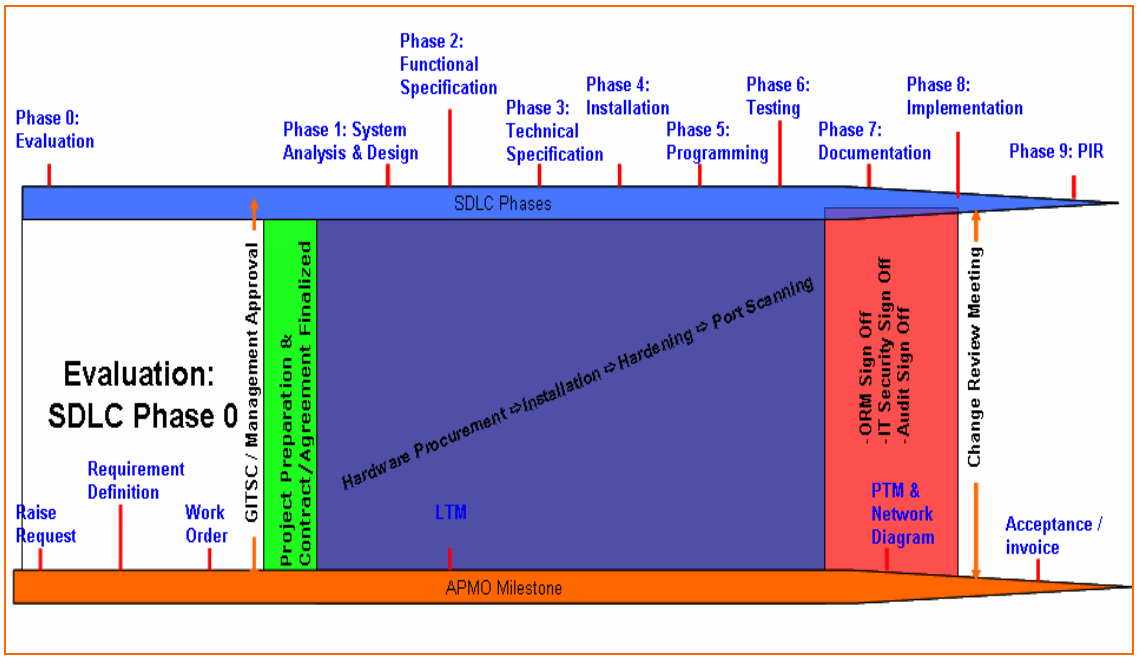

Figure 1.1: Project Life Cycle

The selected case study organization has made the outsource party to be responsible for the infrastructure setup. The APMO process starts from a user to raise their requirements through a formal service request. Then, the representative from the organization, which is the Project Manager will discuss with the representative from the outsource partner company in coming up with the Requirement Definition (RD) or Draft Requirement. Once the RD is confirmed and agreed upon both parties, the Work Order (WO) will be produced. WO is a documented requirement with a stated cost to develop or materialize the request. In this organization, a software assessment and vendor selection will take place during the SDLC phase 0. The activity during this phase is very crucial in order to ensure potential software that was installed during the project implementation is the ideal solution and able to support the business innovation and goals. These processes are important to relate to software evaluation processes because the effort and the cost should be estimated up front or at the beginning of evaluation exercise.

1.3 The Background of the Problem

Annually, the Information System (IS) sector is mandated with at least 400 projects for implementation. These projects are required to support and align the business objective. The directive is critical due to aggressive competition among the Financial Institution (FI) Sector. Each FI desire to come up with own product within the reasonable time frame. Lapse in 'time to market' of the product will dampen the business objective and possibly losing opportunity to the other FI. Even though, the volume of a project is filtered every year whereby only a high Return on Investment (ROI) project is implemented, yet the volume is still far ahead with a comparison to the available manpower. In this case, we are specifically referring to the staff responsible in guaranteeing that the IS Security Policy is followed and being addressed accordingly.

The potential software for implementation in the organization is evaluated through a standard process flow where all participated vendors are having equal chances in providing their solution capabilities. Vendors will need to submit proposal as per requirement and later short listed to present their solution to the organization. IS Security personnel is expected to participate in all evaluation projects and must ensure that the projects implemented are complying with IS Security Policy. Unfortunately, in a big organization with an average of 400 projects per year, it is daunting tasks to ensure software implemented is fully complying with the available policy. The current predicaments that the organization is facing would be:-

1.3.1 Lack of Compliances to IS Security Policy

Occasionally, the projects implemented and systems installed are not able to fully comply with the IS Security Policy and Requirements. Prior to project implementation, evaluation committee was formed in order to evaluate the suitable solution. The solution selected must be able to fulfill the business requirements. Even though the selection of vendors is going trough a very detail and structured process, there are still possibilities that the system is not able to fully comply with the IS Security Policy once the software is installed. This is due to the fact that the committee members is not normally put a priority to other requirement such as security requirement as compared to their business or functional requirement. During the evaluation process, verification is done through a paper based. This is where the proposal submitted is reviewed by the evaluation team. The evaluation committee's decision will be based upon the proposal in which the information is weight from the document and then analyze for further assessment. If it involves such a high investment, the committee may ask participated vendors to prepare a test environment where a "near-production-setup" can be shown to the committee.

Actual verification through a proper set up or a "near-production-setup" is very expensive. Many vendors cannot afford to have this kind of environment. This limitation could caused the software installed may not fully comply with IS Security policy and requirements. Sometimes the non-compliance issue may have been overlook and assume complied by the team due to different understanding within the same subject. Vendors can claim everything is complying with the policy requirement during the evaluation phase in order to win the bid. However, later they failed to do so during the implementation.

1.3.2 Staff Constraint

IS Staff is expected to support the organization business objective by successfully implementing a new software and technology. The technology is an enabler to the organization goals and objectives. Every year, the number of projects waiting to be implemented is very high. IS Security personnel are playing a vital role in order to ensure the software installed is in compliance to the organization IS Security Policy and Standard. A realistic number of people are required to handle tremendous number of projects implemented in the organization. However, the existing manpower is not sufficient and may not able to work efficiently and effectively to support the current needs. Security requirements is the responsibility of everyone in the organization and it is not the responsibility of IS Security personnel alone.

1.3.3 Cost

There is potentially a high possibility to incur additional cost in getting the vendors to comply with IS Security Policy. During the project implementation, it is the responsibilities of the Project Manager to ensure the software installed is comply with the IS Security Policy. Unfortunately, there are cases whereby during evaluation it was noted as comply but it is not able to comply with it when comes for actual implementation. This misunderstanding does happen and could cause the organization to incur with more effort and money to get the system comply with the stipulated policy.

Secure Software Assessment Model (SSAM) needs to be introduced to the selected organization in order to overcome the above shortcomings. SSAM can ensure the process of achieving IS Security compliance through self-assessment by the vendors,

solution providers and the users themselves. The organization would only need to verify the self-assessment from the vendors' responses. However, as mentioned earlier in this chapter, the outcome of the end product by using the assessment model may not guarantee 100% compliance to the security policy, but it can anticipate for the organization on the software assurance compliance level prior to the deployment.

1.4 The Objective

The selected organization for the case study has established a software evaluation process and known as SDLC Phase 0. During this phase, it requires the project evaluation team to produce a documented requirement or Request for Proposal (RFP). The RFP then submitted to the potential vendors or the solution providers. This paper is going to discuss on the above process in more detail in Chapter 2. Even though IS Security personnel is expected to get involve in all evaluation projects, it is extremely difficult to manage the project effectively and efficiently in term of monitoring the security compliances. Hence, this study is formulated to:-

a. Understand the areas of a secure software assessment, particularly areas related to the selected case study organization behavior;
b. Develop appropriate Secure Software Assessment Model (SSAM) which consists of IS Security Requirement Baseline as a simple tools;
c. Integrate the Secure Software Assessment Model (SSAM) to the existing SDLC Phase 0 (Evaluation phase) in the organization; and
d. The success in this integration will result to a prototype of Secure Software Assessment Model.

There are many threats to user's computer, ranging from remotely launched networks services exploits to malicious code spread through emails, malicious code, and file

downloads. Vulnerabilities in IT products are discovered on almost daily basis. Though, it is impossible to ascertain a 100% non-vulnerabilities product, but to a certain degree, assurance is a likely method to reduce the known threats and vulnerabilities in any IT Products. Software Security Assurance is the process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects. (Wikipedia, 2007 Wikipedia. Retrieved October 2007, from http://en.wikipedia.org/wiki/Software_Security_Assurance). By having SSAM, the organization is hoping to achieve the following:-

a. Provide a better snapshot on the level of IS Security Policy Compliance on the intended software installation or intended project implementation;
b. Sufficient and efficient in monitoring project evaluation; and
c. Reduce the risk of extra cost incurred, due to additional scope or add-on in order to comply with IS Security Policy;

1.5 Scope

1. The project scope is only covers to the organization head office located in Kuala Lumpur, Malaysia. It is important to note that the organization has about 22,000 employees and more than 500 branches nationwide. However, the scope of this study is mainly covering a software acquisition by the IS Sector.
2. The main custodian of the process would be the IS Security Department. However, the baseline requirement will be the responsibility of each evaluation project team to update in accordance to their current needs and situation.
3. The scope for this analysis and implementation is to focus on the activity of the Organization's SDLC Phase 0. Detail activity on SDLC Phase 0 will be discussed later in Chapter 2.

4. The development of Secure Software Assessment Model (SSAM) will be based on the organization's IS Security Policy and the development of Information Security Baseline Requirements. The selected policy available are as below:-

Information Security Policy	
1. IS Security Policy	2. Policy on General Systems Security and Controls on ID and Password
3. Security Policy for Overseas Branches	4. Local Administrator Policy
5. Notebook Policy	6. Desktop Policy
7. Anti Virus Policy	8. Internet Usage Policy
9. Firewall Policy	10. Email Usage Policy
11. Enterprise Security Network Architecture Policy	12. Wireless Communication Policy
13. Database Policy	14. Remote Access Policy
15. VPN Policy	16. PKI Guideline
17. Encryption Policy	18. Backup Policy

Table 1.2: IS Security Policies

Currently the organization is enforcing about 18 policies of IS Security. It is not the entire policy requirement is included in the baseline, however most of the critical requirements from the policy are reflected in the checklist. Hence, the baseline requirement is capable to act as the reflection of the organization's policy. By having the baseline requirements, the organization is only required to give out the baseline to the "outsiders" without revealing the internal policy. Through the baseline requirement, vendors who participate in the organization

tender must response to the queries. The IS Security baseline (As per Appendix A) can always be updated with a proper versioning control in place.

1.6 Project Importance

The proposed SSAM is expected to establish visibility and manageability of software installed within the organization. The benefits would be:-

1. Detection of a problem to the current infrastructure, design, policy, and setup.
2. Risk clarification and prioritization on the mitigation process can be done in order to support business objectives; and
3. Increase the understanding of threat and vulnerabilities to the potential product implement at the organization.

1.7 Project Plan

In order to achieve the desired result, figure 1.2 below conceptually lay out major activities to be performed for project completion. The key activities are divided into 4 phases as below:-

Phase 1: Project Identification and scoping

Phase 2: Literature Review and relevant documents

Phase 3: Model Analysis and designing the IT Security Baseline

Phase 4: Pilot Implementation

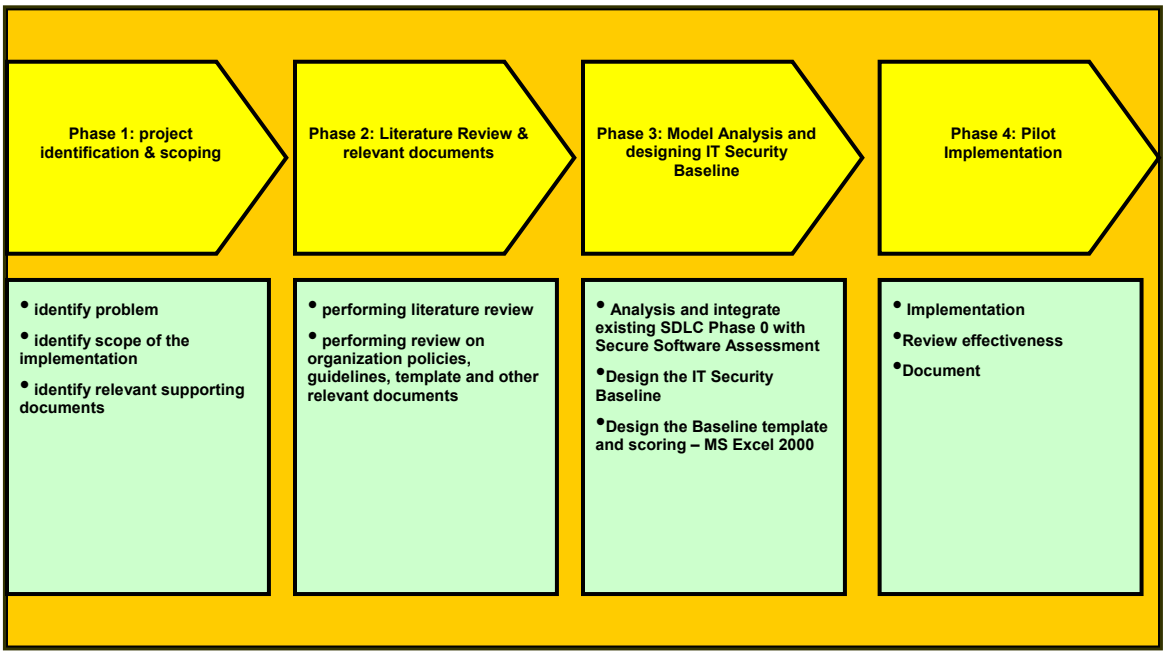

Figure 1.2: Project Activities

1.8 Summary

.

Software Assessment is mostly regarded as decision making on Information Technology investment. Unfortunately, a selection process on the "to be implemented" investment proposal is not straightforward as it may seem. The planned activities on the evaluation or assessment are initiated to manage conformance in term of business requirement, technical requirement as well as security requirement. As per selected organization in the case study, SDLC Phase 0 is the main framework use to initiate the outcome. Software Assessment or Evaluation is defined as the assessment of software product's characteristics in accordance to the specific procedures. During the assessment, the fit or criteria between the software product and the organization needs of that product must be determined upfront. This fit concerns both explicit and implicit needs about the product. This paper presents a proposed software evaluation model with security in minds. The outcome of the end product from this evaluation or assessment model may not guarantee a 100% of compliance to the security requirements. However, it might be able to pre-empt the organization on the assurance level for compliance before the software is deployed. In addition to that, risk mitigation can be done at this juncture to minimize the cost due to non-conformance product.

REFERENCES

Alan W. Brown and Kurt C. Wallnau (1996). A Framework for Systematic Evaluation of Software Technologies. 5-40. Software Engineering Institute, CMU, 19996

Ann Brown (2005). IS Evaluation in Practice. 169-178. The Electronic Journal Information Systems Volume 8 Issue 3.

David Carney (1998). Evaluation of COTS Product: Some Thoughts on the Process. 1-7. SEI Interactive 9/98.

Dieter Gollman (2006). Computer Security. 170-184. (2nd Edition) John Wiley and Sons Ltd.

Federic Copignneaux and Sylvain Martin (1998). Software Security Evaluation Based on a Top down Mc Call like Approach. 414-418. French Ministry of Defense.

Ha Lin, Ahh Lai and Rebecca Ulrich (2006). COTS Software Selection Process. 8, 12-14,18. Sandia National Laboratories.

John Kelsey (2005). Voting System Testing and Evaluation. 1-16. NIST, Computer Security Division.

John Rushby (1995). Formal Methods and their Role in the Certification of Critical Systems. 9-38. FAA Digital Systems Validation Handbook.

Lawrence G. Jones and Rick Kazman (1999). Software Architecture Evaluation in the DOD Systems Acquisition Context. 1-6. SEI Interactive.

Michael S. Bandor (2006). Quantitative Methods for Software Selection. 1-13. CMU/SEI-2006-TN-026

R. Kazman, Mark Klein and Paul Clements (2000). ATAM: Method for Architecture Evaluation 3-15. SEI: CMU.

Ray C. Williams, George J. Pandelious and Sandra G. Behrens (1999). Software Risk Evaluation (SRE) Method Description. 33-59, 73-81. Software Engineering Institute, CMU, 1999.

Syntegra (2006). Common Criteria. Common Criteria Project Sponsoring Organization, May 1998

Teade Punter, Rini van Solingen and Jos Triekens (1995). Software Product Evaluation. 3-10. Eindhoven University of Technology, Faculty of Technology Management, section Information and Technology.