"I/~~We~~ hereby declare that I/~~We~~ have read this master project report and in my/our opinion this master project report is sufficient in terms of scope and quality for the award of the degree of Masters of Software Engineering.

Signature   :

Academic Supervisor   : Dr. Mohd. Naz'ri Mahrin.

Date   : 07/08/2012

Signature   :

Industrial Supervisor   : Siti Sarah Binti Zainal Abidin

Date   : 07/08/2012

TESTING AND BUG FIXING OF

THE INFORMATION SECURITY MANAGEMENT SYSTEM

OMID VAHDANI

A master project report submitted in fulfilment of the

requirements for the award of the degree of

Master of Software Engineering

Advanced Informatics School

Universiti Teknologi Malaysia

August 2012

DECLARATION

I declare that this master project report entitled "*Testing and Bug fixing of the Information Security Management System*" is the result of my own work and research except as cited in the references. The master project report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	
Name	:	OMID VAHDANI
Date	:	07 August 2012

DEDICATION

This master project report is dedicated to my beloved parent, wife and the rest of
family,
and friends in mse-ft-04 batch.

ACKNOWLEDGMENT

Praise to the Most Gracious and Most Merciful, I am grateful to God for blessing me with a successful life and giving me strength to increase my academic knowledge to reach this point.

Having this opportunity I would like to express my special gratitude to my academic supervisor Dr. Mohd. Naz'ri Mahrin for his guidance in writing this thesis, prompt respond to my messages and requests and helping me in understanding the software engineering concepts. Thanks to all lecturers in Advanced Informatics School for their effort in helping me to complete the study in Master of Software Engineering.

Besides, I would like to appreciate my industrial mentor Mrs. Siti Sarah Binti Zainal Abidin and Mr. Farhang for their patience in helping me learning new software engineering technique during the industrial attachment.

My great appreciation to my parents, wife and all my family members for their encouragement and continues support and also to my dear classmates mse-ft-04 group, Atabak, Olfat, Lalitha, Jalal, Abubakr, Ghazal, Sajjad and Abdulrahman who have been working together as a family during this course.

ABSTRACT

The increasing complexity of today's software applications has created a need to do more testing and fixing the problems in the software in order to deliver the final release of the software with an acceptable level of quality. Testing and fixing the problems in software never ends and developing a software application without conducting a sufficient amount of testing and in a systematic way is likely to cause failure of the released product. The aims of this project are to test the Information Security Management System (ISMS) tool developed by SCAN associates Berhad. and to fix the detected problems in the ISMS tool. The methodology of this project includes test plan, designing and implementing the test cases, evaluating and reporting the test, locating and fixing the detected problems and retesting the software in order to find the problems that might be produced because of changes to the code. This project concludes with a new version 2.1.1 of ISMS tool with reports of testing, numbers and areas of passed and failed test cases and report of the detected and fixed problems, and modified files in the software. In this project all of the reported problems from failed test cases were successfully resolved and the final product was delivered to the SCAN company.

ABSTRAKT

Penggunaan perisian yang makin kompleks telah mewujudkan keperluan untuk menguji dan membetulkan perisian supaya perisian yang berkualiti boleh disampaikan kepada pengguna. Pengujian and pembetulan perisian adalah proses yang berlarutan dan aplikasi perisian yang disampaikan tanpa pengujian dan pebetulan yang sistematik dan cukup berkemungkinan besar menghadapi kegagalan yang besar. Tujuan projek ini adalah untuk menguji dan membetulkan Sistem Pengurusan Keselamatan Maklumat (ISMS) yang dibangunkan oleh SCAN Associates Berhad. Metodologi bagi menjalankan projek in adalah melalui pelan ujian, mereka bentuk dan melaksanakan kes-kes ujian, menilai dan melaporkan ujian, mencari dan menetapkan masalah yang dikesan dan ujian semula perisian. Melalui projek ini, versi baru ISMS 2.1.1 dengan laporan pengujian, kes-kes ujian yang lulus dan gagal, fail-fail perisian yang dibetulkan telah disampaikan. Dalam projek ini, kesemua kes ujian yang gagal telah bejaya dibetulkan dan disampaikan kepada SCAN.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AIS : Advanced Informatics School

CMMI : Capability Maturity Model Integration

CMS : Content Management System

DMS : Document Management System

HR : Human Resource

ICT : Information and Communication Technology

IIS : Internet Information Service

ISMS : Information Security Management System

LAN : Local Area Network

STP : Software Test Plan

UTM : Universiti Teknologi Malaysia

WAMP : Windows, Apache, MySQL, PHP

LIST OF APPENDICES

CHAPTER 1

PROJECT OVERVIEW

1.1   Introduction

This chapter provides an overview of the project "A Methodology for Testing and Bug Fixing of the Information Security Management System". This chapter shall describe the background of the company as well as the project background (history and previous versions) during eight months of industrial attachment in the SCAN company. Also, this chapter describes a brief description of the existing problem, and identifies the project objectives and scopes.

1.2   Company Background

SCAN was co-founded by Professor Dato' Dr. Norbik Bashah Idris and nine other co-founders. The Company originated from a research group at Universiti Teknologi Malaysia, which had been conducting research in information security and cryptography since 1996 (SCAN, 2010)

SCAN Associates Berhad ("SCAN"), incorporated on 9 September 2000, is Malaysia`s premier and trusted Information and Communications Technology ("ICT") security solutions provider. SCAN achieved MSC Malaysia Status in December 2002 and was subsequently listed on the MESDEQ market of Kuala Lumpur Stock Exchange on 6 December 2006.

The company currently operates from five different countries, i.e. Malaysia, Indonesia, Saudi Arabia, Syrian Arab Republic and the United Arab Emirates. SCAN has implemented more than RM200 million worth of ICT security projects in Malaysia and overseas. Clients are from various sectors such as the government, banking and finance, telecommunications and oil and gas sectors. In addition, SCAN currently houses the highest concentration of internationally certified ICT security professionals in Malaysia. Moreover, having CMMI level 3 certificate, the company must deliver appropriate services and supports to the clients with the latest edition based on the standard.

1.3   Background of the problem

Development of the Information Security Management System (ISMS software) has been started since 2008 at SCAN. Because, ISMS had initially been developed for governmental organization, therefore delivering a quality product has been important for the company. Moreover, as one of its obligations the company should service its clients according to the CMMI level 3 standard. In addition to the above, SCAN should support the ISMS client (the government) with the newer versions. Therefore, in order to maintain the quality of the software, the ISMS must be delivered with the least possible problems. One of the solutions to this problem is to frequently test the software and fix the problems for every new version that is going to be released.

This project aims to conduct testing the ISMS and fixing the detected problems in the ISMS software.

1.4   Project Background

1.4.1   Introduction to ISO27001: ISMS

The ISO27001 international standard has been prepared to provide a model for establishing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) (ATSEC, 2011).The adoption of the ISMS is the strategic decision for the organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization (ISO/IEC27001, 2005).

1.4.2   Process Approach

The ISO27001 standard adopts the Plan-Do-Check-Act (PDCA) model which is applied to structure of all ISMS processes. Figure 1.1 shows how an ISMS takes input as the information security requirements and expectations of the interested parties and perform the necessary actions to produce a managed information security (ISO/IEC27001, 2005).

Figure 1.1: PDCA model applied to ISMS processes

i.   Plan (establish the ISMS), establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

ii.   Do (implement and operate the ISMS), implement and operate the ISMS policies, controls, processes and procedures.

iii.   Check (monitor and review the ISMS), assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

iv.   Act (maintain and improve the ISMS), take corrective and preventive actions based on the result of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS (ISO/IEC27001, 2005).

As the market gets more competitive and customers become more demanding and sophisticated, it is important for local ICT organisation to implement an organisation-wide information security management framework to give their customers and users greater confidence and assurance.

Consequently, it provides an assurance that the certified organisation has implemented a system for the management of information security in line with an international standard. The organisation is seen to be more credible and serious about information security management, although may not be perfect but demonstrates continues and managed improvement.

ISMS establishes a management framework, which covers the people, IT system and processes within a company. Changes are regularly monitored and reviewed and appropriate actions are taken to improve the security management system. ISMS is part of a company's internal control system by which a company

monitors and controls its security and minimises risks to ensure that it fulfils the requirements of clients, users and partners to deliver products and services in a secure environment.

As a part of SCAN's "ICT" services, ISMS plays a significant role for the company. So SCAN has always endeavoured to improve and release a new update of the tool frequently (SCAN, 2010).

1.4.3 ISMS Background in SCAN

SCAN's ISMS project has begun since 2008. Malaysian government as a client delivers the software to some of its related organisation.

As one of the premier ICT security solution provider, SCAN gives comprehensive consultation in information and communication security based on ISO27001:2005 and ISO27002:2005. To accomplish this objective the company decided to establish a framework by developing an ISMS tools in order to improve the services given to its client. The organisation consulting to SCAN for ICT security solution will now benefit from the ISMS tools to monitor, control and audit the important and valuable property of their organisation.

SCAN's ISMS tool is developed based on the specified ISO27001 requirement and guidance for governmental organizations. Therefore, the design and implementation of the ISMS is influenced by the needs and objectives, security requirements, the processes and structure of the governmental organizations. Since this ISMS tool is supposed to be distributed between several organizations, the ISMS must satisfy a general set of requirement (in accordance to ISO27001) and support the organizations with any type of information security requirement. Based on the given description above, the existing ISMS system's features will be scaled over time in accordance with the needs of the organization. In conclusion several versions of the ISMS have been released so far.

The ISMS project initially aimed to establish a framework to support the management of organisation's areas, processes, assets and risks. The first version of the ISMS software consists of risk management, user and department management and ISMS audit. Being released as the first version of ISMS, it had some deficiencies and poor functionality. Therefore, it could not be considered as a thorough ISMS tool. For example navigation through different parts of the software was difficult and not user friendly, and there was not any dashboard to have a general control over the different parts of the system. So, as a part of company's commitment the ISMS functionality and usability had to be improved.

ISMS Version 2.0 released by SCAN on 2009 with some new features added to the tools. The main features consist of the following:

i. User can now navigate from different parts of the system such as area, process, asset and risk.

ii. Controls over risk management, user management, and department management are now enhanced.

iii. Dashboard added to the system which provides easier access to different part of the ISMS.

iv. ISMS is now integrated with MyRAM (Risk Management software). A link to MyRAM added to the ISMS so that the administrator can import information from MyRAM database.

In 2010 the company released ISMS version 2.1 to keep updating and improving the software. Some new features were added to the new version such as tree view on the dashboard to navigate through risks, areas, processes and assets.

The current version of the project which is now under development has some new functionalities such as:

i. Document Management System (DMS).

ii. Threat Catalogue was added to the system.

iii. Administrator has now centralized control over the ISMS.

Since the beginning of the ISMS establishment, SCAN has attempted to update the ISMS framework by adding new features, fulfilling more requirements and minimizing bugs according to the ISO27001-27002 standard.

1.5   Project Objectives

Based on some problems and weaknesses discussed on current version of ISMS in previous section, this project will focus on testing and bug fixing of Information Security Management System (ISMS) software. To ensure achieving the goal, the following objectives are aimed to be gained:

- To test the ISMS software.
- To evaluate the test results and report the problems.
- To fix the detected problems.
- To conduct the regression testing.

Each step and activity related to that objective will be defined in project scopes and project methodology.

1.6   Project Scope

Testing is conducted in an integrated environment consists of a Linux based main server and four testing machines. Software Test Plan (STP) and Test Description and Report are prepared based on the company's test case form, and requirements stated in the ISO/IEC 27001 standard.

Scopes of testing are including "Document Management System"(DMS) and ISMS under admin view which is "Admin Dashboard". Black box testing will be conducted and functionality of system in unit and system level will be tested.

Regression testing will also be conducted after correction. Test cases are implemented based on the test case form prepared by the company. In addition, ISMS features will be compared to the similar ISMS tools from other companies in order to find and suggest new features to the project manager, but if it complies with ISO/IEC 27001 standard.

For evaluation of the testing activities, we will evaluate the test procedure according to the test plan review checklist and test case form. Scope of the test evaluation and measurement will be based on the set of criteria which are test completeness, test correctness, test traceability, test resources and schedule and regression test. These criteria are described in detail in test plan review checklist (See Appendix A). For analysis of the test result, we will do it based on expected result in the test case form and the testing coverage rate (Traceability table).

To fix the problems defects, bugs and errors will be logged in the test case form. Locating issues will be applied in the source code and tracing issues from source code to design and requirement documents will be done by other project members. Results will be logged through an issue tracking tool integrated with a configuration management tool.

Regression test will be conducted at unit and system level to ensure that system functionalities are sustained and other parts of the system are not affected in result of fixing one part.

Other than the new version of ISMS software as the main deliverable, the following must be provided to the company:

- Software Test Plan (STP)
- Test case description (test case form)
- Reports of the test implementation and detected and fixed problems.

Content of the STP is based on the company's test plan guideline. Test case description and report will be prepared in the test case form. Reports of the reported and fixed problems will be generated from the issue tracking and subversion tools.

1.7 Project Plan

Software Test Plan (STP) document is used as the planning document to describe the step by step guidance to the project goal. The project Gantt chart shown in Figure 1.2 on the next page illustrates the project activities to be performed in this project. Detailed activities of the project plan such as identification of scope, environment, schedule, risk and test execution, reporting, monitoring and completion will be defined in software test plan document. Moreover, the amount, level of detail, structure and templates for the test documentation and test procedures will be described in the STP.

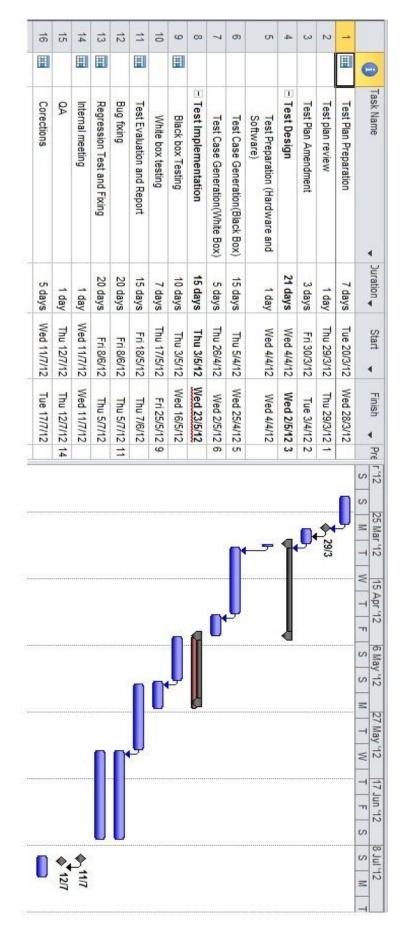|		Task Name	Duration	Start	Finish	Pre
1		Test Plan Preparation	7 days	Tue 20/3/12	Wed 28/3/12	
2		Test plan review	1 day	Thu 29/3/12	Thu 29/3/12	1
3		Test Plan Amendment	3 days	Fri 30/3/12	Tue 3/4/12	2
4		Test Design	21 days	Wed 4/4/12	Wed 2/5/12	3
5		Test Preparation (Hardware and Software)	1 day	Wed 4/4/12	Wed 4/4/12	
6		Test Case Generation(Black Box)	15 days	Thu 5/4/12	Wed 25/4/12	5
7		Test Case Generation(White Box)	5 days	Thu 26/4/12	Wed 2/5/12	6
8		Test Implementation	15 days	Thu 3/5/12	Wed 23/5/12	
9		Black box Testing	10 days	Thu 3/5/12	Wed 16/5/12	
10		White box testing	7 days	Thu 17/5/12	Fri 25/5/12	9
11		Test Evaluation and Report	15 days	Fri 18/5/12	Thu 7/6/12	
12		Bug fixing	20 days	Fri 8/6/12	Thu 5/7/12	11
13		Regression Test and Fixing	20 days	Fri 8/6/12	Thu 5/7/12	
14		Internal meeting	1 day	Wed 11/7/12	Wed 11/7/12	
15		QA	1 day	Thu 12/7/12	Thu 12/7/12	
16		Corrections	5 days	Wed 11/7/12	Tue 17/7/12	14

Figure 1.2: Project Gantt chart

1.8 Chapter Summary

This chapter discussed the overview of the project. Background of the company, fields of activities, structures and software engineering experiences were also introduced. As described, the main problem that this project is going to solve is to test and fix the problem for the ISMS system. Objectives that were identified are, to perform testing the ISMS software, to evaluate the testing and report the detected problems, to fix the detected problems and to conduct regression testing.

Testing will be performed in an integrated environment consists of Linux server and four Microsoft Windows clients as testing stations. Scope of the testing is "DMS" and "Admin Dashboard", black box will be conducted in system level and unit level as well as the regression testing. Detected problems will be reported and solved in the source code. Test plan will be prepared and report of the test design and implementation will be provided in the test case form as well as the reports of the issue tracking and sub versioning tools.

REFERENCES

Anupam.V, F. J. k. L. D., 2000. *"Automating Web Navigation with the WebVCR",* s.l.: Bell Laboratories, 600 Mountain Ave., Murray Hill, NJ 07974, USA.

ATSEC, 2011. *Information Security, ISMS, and ISO/IEC 27001.* [Online] Available at: http://www.atsec.com/us/iso-iec-27001-faq.html#2 [Accessed 12 2 2012].

Avedos, 2012. *Information Security Management System.* [Online] Available at: http://www.avedos.com/en/grc+solutions/information+security+management+system+isms+/information+security+management+system+isms+.html [Accessed 28 2 2012].

Buckler and Craig, 2009. *MySQL: the Pros and Cons of MyISAM Tables.* [Online] Available at: http://www.sitepoint.com/mysql-myisam-table-pros-con/ [Accessed 26 2 2012].

ECC, 2012. *Assessment.* [Online] Available at: http://eccinternational.com/ [Accessed 14 2 2012].

E-COP, 2010. *ISMS-toolkit.* [Online] Available at: http://www.e-cop.net/ISMS-toolkit.html [Accessed 14 2 2012].

Hope Paco and Walther Ben, 2008. *Web Security Testing Cookbook.* s.l.:O'Reilly Media, Inc..

Iftikhar and Javed , 2010. *Performance Testing and Analysis of Modern Web Technologies,* Västerås, Sweden: Mälardalen University.

ISO/IEC27001, 2005. *ISO/IEC27001:2005.* [Online] Available at: http://www.iso.org/iso/catalogue_detail?csnumber=42103 [Accessed 11 2 2012].

ISO, 2012. *No 3 Comprehensive ISO 27001 ISMS Toolkit.* [Online] Available at: http://www.27001.com/products/20 [Accessed 14 2 2012].

JScripters, 2012. *Javascript: advantages and disadvantages.* [Online] Available at: http://www.jscripters.com/javascript-advantages-and-disadvantages/ [Accessed 25 2 2012].

L.Xu and Baowen.Xu, 2007. *Applying Agent into Intelligent Web Application Testing.* s.l., IEEE, pp. 61-65.

L.Xu, B. Z., 2003. *Website Evaluation Based on Statistic Data.* s.l., IEEE, pp. 301-306.

Lei.Xu, X. B., 2004. *A Framework for Web Application Testing.* s.l., IEEE.

Michael Widenius and David Axmark, 2002. *MySQL reference manual: documentation from the source.* Helsingfors, Finland: O'REILLY COMMUNITY FREE.

Microsoft, 2012. *Regression Testing.* [Online] Available at: http://msdn.microsoft.com/en-us/library/aa292167(v=vs.71).aspx [Accessed 28 2 2012].

MySQL, 2012. *www.mysql.com/why-mysql/marketshare/.* [Online] Available at: http://www.mysql.com/why-mysql/marketshare/ [Accessed 26 2 2012].

Newman and Chris, 2005. *Sams Teach Yourself PHP.* s.l.:Sams Publishing.

Nixon and Robin, 2009. *Learning PHP, MySQL, and JavaScript.* s.l.:O'Reilly Media, Inc..

Oracle, 2012. *Internal Locking Methods.* [Online] Available at: http://dev.mysql.com/doc/refman/5.6/en/internal-locking.html [Accessed 24 2 2012].

PrivaTech, 2012. *Information Security Audit.* [Online] Available at: http://www.privatech.ca/privacy-consulting/information-security-audit/ [Accessed 14 2 2012].

Reza Hassan, O. K. M. A., 2008. *A Model Based Testing Technique to Test Web Applications.* s.l., IEEE, pp. 184,185.

SCAN, 2011. *ISO/IEC 27001 Compliance.* [Online] Available at: http://www.scan-associates.net/services_isms.htm [Accessed 13 2 2012].

SCAN, 2010. *Scan Brief History.* [Online] Available at: http://www.scan-associates.net/corp_history.html [Accessed 11 2 2012].

SoftwareTestingHelp, 2007. *Regression Testing with Regression Testing Tools and methods.* [Online] Available at: http://www.softwaretestinghelp.com/regression-testing-tools-and-methods/ [Accessed 25 2 2012].

TortoiseSVN, 2011. *TortoiseSVN's Features.* [Online] Available at: http://tortoisesvn.net/docs/release/TortoiseSVN_en/tsvn-intro-features.html [Accessed 2 3 2012].

verinice, 2012. *Features.* [Online] Available at: http://www.verinice.org [Accessed 16 2 2012].

Wircken, J., 2011. *Facts About Php Programming Language.* [Online] Available at: http://www.phpdc.org/Facts-About-Php-Programming-Language.html [Accessed 3 3 2012].

Yang, 2009. *MySQL Engines: InnoDB vs. MyISAM.* [Online] Available at: http://www.kavoir.com/2009/09/mysql-engines-innodb-vs-myisam-a-comparison-of-pros-and-cons.html [Accessed 5 3 2012].