TESTING INFORMATION SECURITY MANAGEMENT SYSTEM TOOL V2.1.1.0 BASED ON ISO 27001:2005

Abdulrahman Mustafa Shehu

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

ABSTRACT

Every single day software engineers are born with new talented skills and logics. They all engage in developing sophisticated systems that will affect the life of the intended users in either positive or negative ways. It was also surprising to know that recently even a 13year old Pakistani was able to break the record of been the youngest Microsoft certified professional (MCP). Some are saying that doctors are more important to the society than all other professional bodies but the way the world is moving we can say software engineers can have equal or even more importance to the world today. Having this entire competitive platform in our mist, it is very important to give maximum effort and consideration to the testing of developed systems. Although engineers at large cannot test their products to a point of saturation, they will try to make it by anticipating situations where it might possibly fail, producing dedicated verification and validation terms and other different ways. Usually, the time allocated to testing activities is limited as the producers are eager to send the product to the client side and collect the remaining contract balance. This report aimed at exploring the concept of information security management system (ISMS) and the tool used to automate the implementation of ISMS by monitoring organisation's ISMS compliance. A complete standard was provided to guide in the requirements to implement ISMS which is ISO 27001. The standard envelope the establishment, implementation, operation, monitoring, review, maintenance and improvement of ISMS. This states how vital it is to conduct thorough testing on the tool to ensure an error free system is used to manage the delicate task of managing important information. The report highlights all the testing activities carried out on the delicate tool to regain its standability and strength.

ABSTRAK

Saban hari jurutera perisian didedahkan dengan kemahiran dan logik terkini. Mereka sentiasa terlibat dalam membangunkan system canggih yang mempengaruhi kehidupan manusia baik dari segi positif atau negatif. Baru-baru ini dunia digemparkan dengan berita remaja Pakistan berusia 13 tahun berjaya memecahkan rekod sebagai pemegang anugerah Microsoft Certified Professional (MCP) termuda. Ada yang mengatakan doktor adalah pekerjaan paling penting dalam masyarakat, namun dengan peredaran zaman, tidak dinafikan bahawa jurutera perisian juga mempunyai peranan yang penting masa kini. Oleh itu, adalah penting bagi kita menilai semula dan menumpukan fokus kepada pengujian terhadap system yang dibangunkan. Walaupun jurutera perisian tidak mampu menguji keseluruhan sistem, mereka akan memikirkan situasi-situasi yang berupaya menyebabkan sistem gagal dengan menghasilkan scenario khusus bagi setiap fungsi. Biasanya masa yang peruntukkan untuk proses pengujian adalah begitu terhad disebabkan faktor pembekal yang ingin menghantar sistem dalam masa yang singkat demi mengejar bayaran awal. Laporan ini bertujuan meneroka konsep pengurusan sistem maklumat sekuriti (ISMS) dan penggunaan perisian bagi tujuan automasi perlaksanaan ISMS dengan cara penilaian pematuhan organisasi terhadap piawaian tersebut. Piawaian lengkap dibekalkan dengan panduan keperluan melaksanakan ISMS berdasarkan ISO27001. Piawaian ini memperincikan penubuhan, pelaksanaan, operasi, penilaian semula, penyelenggaraan dan penambahbaikan ISMS dalam organisasi. Ini menunjukkan betapa pentingnya pengujian teliti dilaksanakan ke atas perisian iaitu bagi memastikan sistem bebas dariada kesilapan dalam pengurusan maklumat penting. Oleh itu, laporan ini menegaskan aktiviti pengujian yang dilaksanakan ke atas perisian ISMS untuk menghasilkan perisian yang stabil dan mempunyai daya tahan yang tinggi.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ISMS	-	Information security Management System
ISO	-	International organisation for standardization
ICT	-	Information and communications technology
MyRAM	-	Malaysian Risk Assessment Management
INFOSEC	-	Information security
PDCA	-	Plan Do Check Act
IDE	-	Integrated Development Environment
WYSIWYG	-	What you see is what you get
SME	-	Small and medium enterprise
SOA	-	Statement of applicability

CHAPTER 1

PROJECT OVERVIEW

1.1 Introduction

This chapter describes a brief overview of the project to give the reader a picture of what we are dealing with. The chapter will be covering the section of company background, project background, project objectives & scopes and with the final sections highlighting areas on the importance of project and summary of the whole chapters.

1.2 Company Background

SCAN Associates Berhad (SCAN), is one of the lead and trusted ICT security solution contributors in Malaysia. It is a company affiliated to a very sound company known as commerce Asset Ventures Sdn. Bhd., which is a company totally owned venture capital arm of Bumiputra-Commerce Holdings Berhad (Bhd, 2007).

It is a company with sound track record of providing ICT security solutions and structuring its intellectual property, Scan is recognised internationally by delivering standard solutions and services around the globe.

To extend ICT to its elastic limit, SCAN is supported by different sectors of Malaysian government agencies that include the Multimedia Development Corporation and Malaysian Dept Ventures which aim is to spread ICT security initiatives to all corners of Malaysia and overseas. Currently, SCAN associates have in its possession the highest concentration of internationally certified and skilled ICT security professionals in Malaysia.

As a company dealing with security issues, the main target of the company is to uphold trust and security of information for its valued customers. It also provides the optimum customer-centric solutions and services to the growth of regional and global market and they target to be the leading global ICT security solution providers (Bhd, 2007).

1.2.1 Brief History

SCAN was originally founded by a talented and versioned man named by Professor Dato' Dr. Norbik Bashah Idris. The co-founder together with nine other co-founders kick off from a research group at Universiti Teknologi Malaysia which had been conducting research in Information security and cryptography since 1996.

Since its foundation, SCAN succeeded in earning reputation from different kind of companies and partners. It was later appointed the ICT consultant to the Malaysian Government in 2000 and has since built a strong track record in both the public and private sectors. The company have different kinds of clients from Malaysian government, banking and finance sectors to telecommunication and Oil & gas sectors (Bhd, 2007).

1.2.2 Vision and Mission

SCAN has its own vision which aims to become a global, world-class and trusted ICT security Solutions Provider. Its mission is to be a dedicated team of professionals that shall add value to their clients in responsibly securing their ICT infrastructure by using the best technology, processes and innovative solutions as well as delivering world-class expertise in accordance with international standards.

1.2.3 Strengths and Competitive Edge

SCAN makes maximum use of information and communication technology and particularly in ICT security technology with providing ICT Security solutions and services (Bhd, 2007). The solutions and services that is rendered by the company consist of the following

a) Information Security
b) Communication Technology
c) Network security

1.2.4 Research and Development

SCAN is involved in different kinds of research and development activities in the area of ICT security.

a) Vulnerability research works
b) Network Surveillance
c) Cryptography
d) SCAN collaborates with various universities and other organisations in R&D.

1.3 Background of the problem

Information security management system (ISMS) project was first started in 2008 to provide secure way of managing information to its clients. As known that Scan associates is a company that is specialised in information and communication technology (ICT) and it's a security provider accredited by Malaysian government. Mostly all the projects handled by the company are government project which shows that information leakage is the least to be expected. Information leakage in a company points out that security measures are not implemented. This raised alarm of implementing ISMS project according to ISO 27001 standard. ISMS was put into place to establish policies, objectives and controls information security within the framework of organisations overall business risk.

The first version of ISMS contains some functionality such as the dashboard, risk management, reports and the admin section. This was reported not to cover all the requirements specified by ISO/IEC 27001 and ISO/IEC 27005. In 2009, the company decide to work on releasing an upgrade to the version previously released. This new version comes with easy navigability for users on the system and a dashboard view. Later the company released version ISMS 2.0 that includes functions that are previously not part of the system. Functions like importing information from a sister system called MyRAM (Malaysian Risk Assessment Management). Working on the new release came into action in 2010 where data management system and threat catalogue was included. The enhancement came in parallel with working on the bugs discovered in the previous version.

This project is intended to be fully functional according to the standard by the end of the industrial attachment.

1.3.1 Benefits of ISMS

A company having in its possession a certificate of ISO/IEC 27001 shows that it has adapt and maintain a documented ISMS that revolves around the principle of Plan-Do-Check-Act. The core benefits of ISMS include;

a) It provides a framework for the company to comply with regulatory/legislation requirement,
b) It strength the bond of trust among present and potential clients from the marketing point of view,
c) It also ensures that your company complies with the industries best practices for security.
d) By complying with the standard, a better work exercise and ethics in security is established.

Scan associates decide to implement this project to help other companies meet the compliance of ISO/IEC 27001 goals in shortest time and reduced cost.

1.4 Project Objectives

The system in question is an automated system to manage the information security in companies that information is very sensitive and to control information security as well as Risk management. Therefore, after identifying and modelling the requirements into a well structured design, some group of team members proceed with implementing into a web application form. During the period of Industrial attachment, the author is expected to meet the following objectives;

a) To conduct testing on ISMS tool
b) To document the test result for testing
c) To perform correction based on the test results

d) To add new features that are requested by the company

1.5 Project Scope

The above listed objectives can be achieved by following some specific scopes. These scopes are divided base on industrial attachment 1 and industrial attachment 2 for a more organised as well as easy tracking of improvement.

I. Industrial Attachment 1 (IA 1):

a) To engage in practicing PHP and MySQL using text books and all possible resources
b) To test the Dashboard of the ISMS tool for any bug
c) To create an organised test plan on how the testing activity will be conducted
d) To engage in fetching out articles related to the topic in question (ISMS)
e) To use tortoise SVN software in managing the modification made on any part of the system.

II. Industrial Attachment 2 (IA 2):

Some of the scopes will surely be in the IA 2 because it will be continues process. These include fetching and reading of articles on ISMS, engaging in reading and practicing PHP & MySQL reference book and using tortoise SVN for configuration management. Some new scopes that need to be achieved during this period to fulfil the required task include;

a) To test other parts of ISMS tool that include Risk Management, Report section and profile
b) To develop the documents on testing

c) To test the functionality of the ISMS tool base on white box, black box and grey testing
d) To familiarize with PHP and MySQL platforms to be able to carry out unit testing
e) To implement and correct the bugs encountered during testing
f) To implement new features that will allow administrator to register different companies to the ISMS tool

1.6 Importance of the Project

The ISMS project is vital to the company because of it engulf a number of potential benefits to the company. Some of the benefits the company will gain by managing and maintaining this project may lead to achievement of company's objective to be a world class security provider. By implementing this project, the company will have guarantee business continuity while minimizing business damage. It will also ensure that the company maximize the investment returns and opportunity for its business. The company will be able to maintain competitive edge as well as ensure smooth commercial image among its clients. By implementing ISMS correctly it can decrease the impact on the company's business of a breach of security, lost productivity, increased labour costs for repairs and lost brand equity. Above all, ISMS project is a very delicate and vital project to the progress of the company and betterment of services.

1.7 Project Report Outline

Chapter 1: This chapter provides the reader a hint of what the thesis is all about and shades light on the background of the company in which the project is managed. It also outlines the objectives that are expected from the author to be achieved during the period of industrial attachment.

Chapter 2: This chapter will provide a thorough research on the topic of the project while bringing out the best works that is related to the project which are already implemented. More so, the author will create a means of critical analysis between the systems out there and the system under construction to find the gap that needs to be patched up. Review on the tools that can possibly be used during this process will also be covered under this chapter.

Chapter 3: Talking about the methodology that will be used to test the system. This chapter will describe the testing process from test plan to bug fixing according to IEEE STD of testing and documentation.

Chapter 4: The process of testing, bug fixing and implementation of new features will be detailed out in this chapter showing how every step is carried out.

Chapter 5: The conclusion of the whole exercise that was done in the previous chapters will be put to a hold in this chapter. It will also provide future recommendation and lesson learnt during this interesting and hectic period of attachment.

1.8 Chapter summary

This chapter provides a brief insight of the company the author is attached to for the period of the industrial attachment. It states the kind of activities that are practiced by the company and the kind of task the author is assigned to which will cover the scope of the thesis. The objectives the author is supposed to meet and scope of those objectives are described in details for the leaders' clarity.

The chapters below which include literature review, project methodology and the rest will give a detail breakdown of the backbone of the thesis. Before going deep

into the project in question, the author took ample amount of time to research on the related topic and all the associated components that are linked to the project. The next chapter will be highlighting the thorough research made by the author.