ICT SECURITY POLICY COMPLIANCE SYSTEM: IMPLEMENTATION

Mohd Farizul Mat Ghani
School of Science and Engineering,
Malaysia University of Science and Technology, Selangor, Malaysia
Email: farizul.ghani@moe.gov.my

Sellappan Palaniappan
School of Science and Engineering,
Malaysia University of Science and Technology, Selangor, Malaysia
Email: sell@must.edu.my

ABSTRACT

As online business transactions become more pervasive, ICT security has become a major concern today. Many organisations are beginning to realise the need to protect their IT assets both from accidental disasters and malicious or intentional attacks. IT Security is a fundamental requirement. How organisations safeguard and protect their assets depends on the availability of resources and decision-making capability. As ICT security policy is so important, it is often the subject of discussion in the public sector. Most of the security breaches occur in government departments that offer online services to the public. That includes the Marang District Council (MDC) IT Department (BTM) as it also provides services to the public. Based on research findings and from feedback gained from the Marang District Council, these security breaches can be reduced by providing a comprehensive computerized ICT Security Policy document guideline. Besides creating user awareness, the guideline can be used to enforce the policy.The purpose of this research is to investigate and resolve problems related to the implementation of the ICT Security Policy at the Marang District Council. Specifically, it will include the design and development of the policy system that will assist the Information Technology Department (BTM). The IT Department will act as the Marang District Council's ICT Security Secretariat in providing a good and complete ICT security policy [18] document. This will ensure the implementation of ICT security policy in its totality. Besides, these documents will be compliant with the ISO 27001 standard and the Information Technology Security and Communication Policy for the Public Sector that was developed by The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)

KEYWORDS: Policy Implementation, ICT Security Compliance, Security System, Information Technology Security, ICT Security Policy.

1.0 INTRODUCTION

The rapid development of Information Technology in this country proves how fortunate our generation nowadays. As a result, we have a world without boudaries. Information, Communication and Technology (ICT) does not only serve as a communication agent, it also acts as a bridge for user to benefit as part of the routine and the necessities of life.

The security of ICT is closely related to ICT assets and information protection. This is because the hardware equipment and software components that are part of the ICT assets in government organisations are large investments and need to be protected. In addition, the information stored in the ICT system is valuable because a lot of resources are required to produce it and the information will be difficult to be re-generated in a short period of time.

Furthermore, certain information that has been processed by the ICT system is deemed to be sensitive and classified. Unauthorized disclosure or information leakage could harm the national interest. Any usage of government's ICT assets apart from the outlined purpose and intention is considered as misuse of government's resources. ISMS survey which was conducted by **CyberSecurity Malaysia** in the month of October 2014 on 100 organizations had revealed that normal attacks are viruses (87%) and mail spamming (83%). In addition, more than 68% of the organizations have little knowledge on ISMS. Moreover, 37% of the organizations do not have any security policy at all [13].
From time to time, in order to address these risks, Government's ICT Security Policy will be consistently defined through ICT Security Standards which covers guidelines and ICT security measures. The usage of all these documents as an integrated whole is recommended. This is because the formulation of policies, standards, rules, outlines and security measures are oriented in order to protect data confidentiality; information and the conclusion that can be made out of it.

1.1 Problem Statement

It is difficult to fulfill ICT security requirements due to the complexity of ICT systems, which can be exposed to vulnerabilities, threats and risks. ICT systems and its components communicate and dependent to each other often produce various kinds of weaknesses.

However, these risks should be identified and dealt with appropriately. To ensure that the ICT System is secured all the time, ICT Security Policy must cover the safety of all forms of information entered, produced, destroyed, kept, generated, printed, made, distributed, in the delivery and those with backup copies in all ICT assets [15].

1.2 Main Priorities of "ICT Security Policy"

"ICT Security Policy" underscores severalcompelling priorities the implementation of which is necessary to meet the objectives set out in the document.

The first priority of "ICT Security Policy" is to define the strategy in respect of ICT security provision. The Policy provides an overview of those principles that lead to the creation of safe infrastructure and strategies that will serve as a solid basis for safe protection of information systems and networks in Defence Sector. The Policy calls for effective and close collaborative engagements from local structures to facilitate MoDin securing its critical infrastructure.

The second priority is to protect the information systems of Georgian Armed Forcesfrom potentialcyberattacks, develop methods and means for intelligence and radio digital fighting, active confrontation possibilities and psychological operations.

In the light of substantial growth of cyber attacks MoDfocuses on creation of secure and adequate information environment, which is the precondition for stable functioning of ICT infrastructure. MoDis ready to implement all necessary actions for meeting cyber security challenges and to establish a reliable platform for further development of cyber security. Due to the dynamic nature of cyber space, there is now a need to consider all ICT security related issues within the framework of "ICT Security Policy" highlighting an integrated vision and coordinated strategy for implementation.

1.3 Project Goals

The main goal of the project is to implement a system that will help MDC to comply with ICT Security Policy based on ISO 27001 standards, circular and guidelines from MAMPU and set up system will help MDC to implement ICT Security Policy.

1.4 The objectives of this project are as below:

- To conduct a research and build a prototype based on existing ICT Security standards, following the guidelines provided by MAMPU and ISO 27001.
- To obtain information and suggestions on ICT Security Policy from the ICT Security Policy Compliance System (ISPCS) and officers involved in the management of ICT MDM.
- To create and produce documents on ICT Security Policy. This will be used generally for Information Technology Department and specifically for MDM using the developed ICT Security Policy Compliance System (ISPCS).
- Design a mobile application for group expenses.
- To implement the model on a Cross-Platform mobile application.
- Using the developed ICT Security Policy Compliance System (ISPCS).

1.5 Project Scope

- To analyze and review ISO 27001 security standards and Information Technology Security Policy and Communication for Public Sector and the circular issued by MAMPU.
- The research will be carried out towards MDC, Information Technology Division, whom act as MDC's ICT security secretariat.
- ICT Security Policy Compliance System (ISPCS) will be implemented to assist MDC's Information Technology Division to prepare ICT Security Policy documents. To develop this project, PHP and My SQL will be use as the system's database.
- Following are the users of the system, whom will be directly involved in implementing ICT Security Policy:
    a. IT Manager (Information Technology Division)
    b. MDC's IT Officer (Management Division, Information Technology Division and Finance Division).

2.0 LITERATURE REVIEW

Incidents Trends Q1 2014

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign, which include home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on several cyber incidents.

From January to March 2014, MyCERT, via its Cyber999 service, handled a total of 3143 incidents representing 4.40 percent decrease compared to Q4 2013. In Q1 2014, incidents such as Denial of Service, Fraud, Vulnerabilities Report and Malicious Code had increased while other incidents had decreased.

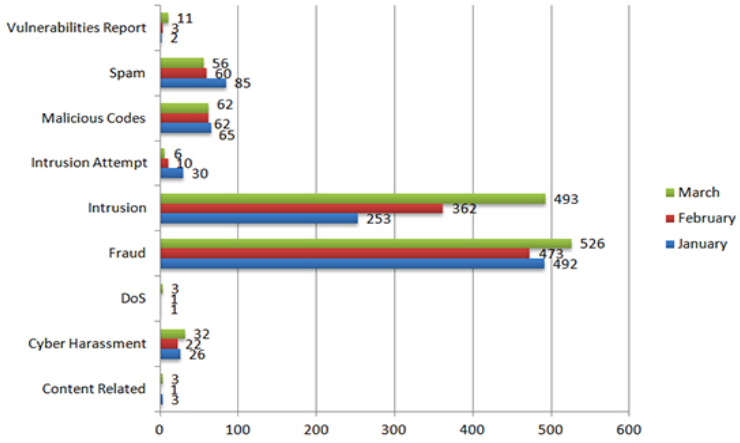

Figure 1: Illustrates incidents received in Q1 2014 classified

In Q1 2014, a total of 1108 incidents were received on Intrusion representing 18.34 percent decreased compared to previous quarter. The Intrusion incidents reported to us are mostly web defacements or known as web vandalism followed by account compromise. Based on our findings, majority of the web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache.

In this quarter, we received a total of 689 .MY domains defaced belonging to various sectors such as private and government hosted on local web hosting companies. MyCERT had responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations. Figure 2 shows the breakdown of domains defaced in Q1 2014.

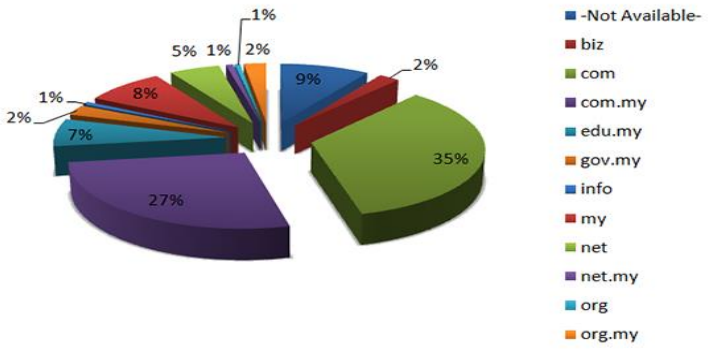

Figure 2: Shows the breakdown of domains defaced in Q1 2014

Information Communication Technology (ICT) Security Policy

According to Dr Mingu Jumaan, Director of state Computer Service Department said that ICT Security Policy needs to be defined to protect the government ICT assets as well as to provide better and faster response to security incidents. Hence, poor ICT security can leads to inability to function and lose of data, incur more cost to fix and recover data, disruption to government operation and damage reputation. Thus, the Department of the Prime Minister Malaysia is reported that the ICT Security Policy is designed to meet the needs of enforcement, control and comprehensive measures to protect assets government's ICT.

ICT Security Compliance

The ICT security compliance can be define as comply with all procedures or regulations. Douglas and Wildavsky (1982) claimed that complying with all rules in the policy understand the responsibility of the task, especially related to ICT as well as not doing things that can damage the ICT tools or expose the organizations information. A guideline by ICT Security Policy, 2009 also state the type of disciplinary action which may be made to staff who violate the rules.

3.0 DATA ANALYSIS

This chapter will discuss the analysis of the data and information collected from the questionnaire comprising of 19 questions. The data and information collected were verified, edited and then analysed to match the objectives of this research.This includes the information on the components in the ICT Security Policy Compliance System (ISPCS) architecture and modules available to the user. Based on the architecture, the requirement analysis and detailed design of the ISPCS were then carried out.

3.1 Data

Primary data is used for this research and the data is obtained using self-administered questionnaires. The questionnaire comprised of six sections. Section 1 is designed to capture the respondents' demographic. The questions asked in this section are related to respondents' type of department, gender, age group and educational level. Then, for Section 2 until Section 5 is design to measure the staff responsibility of independent variable (Development and Maintenance Policy, Management Policy, Security Policy and Access Control Policy respectively) towards ICT Security Compliance among staff. Section 6 is designed to measure the ICT Security Compliance among staff.

3.2 Population and Sample

The population of study is defined as the all staff at Marang district council (MDC) Terengganu who involved of ICT. The sample of study is 150 staffs at MDC who involved of ICT. The rule of thumb for determining sample size which appropriate for most research is sample should be larger than 30 and less than 500. (Sekaran, 2003). The study used Stratified Sampling Technique where the population divide into 2 subgroups called strata that are male staff and female staff. Then both of strata are divided according to the type of department which are Division Department. Randomly selected sample from each stratum to collect the respondents and take the respondents from each stratum using the lucky draw method.

3.3 Result

Out of 150 respondents, 75% of them are male while the remaining 35% are female. Majority of the respondents are working at Administration and Information Technology Division with 62% and another 38% of the respondent are working at Treasury and Finance Division. For the Unit, most of respondents which are 10.5% from Engineering Unit and Town and Country Planning Unit while only 0.9% of respondents are from Irrigation Unit. Then, for the division, majority of respondent are from Hydrology and Water Resources Division (BHSA) which is 7% while only 1.8% of the respondent are from Division of Management Services (BKP). 62% of the respondents aged between 31-40 years and another 23% of the respondents aged between 20-30 years. While, 13% of the respondents aged between 41-50 years and the remaining 2% is between 51-58 years.

Furthermore, 45% of the respondents are Diploma holders and 37% of the respondents are SPM holders. Another 11% of the respondents are Degree holders and 5% of the respondents are STPM holders. The remaining is 2% of the respondents are Certificate and Matriculation holders.

4.0 METHODOLOGY

This chapter consists of project design, project development. In further study, research and understanding of the previous system must be consider in order to come up with the good and appropriate project plan and design.

4.1 Project Design

The succeeding methods include the development of the system. Information is provided to show the association of work and function of the proposed system. The following figures illustrate the flow of the system.

In functional decomposition diagram, all the processes are shown. In ICT Security Policy Compliance System (ISPCS), the enterprise components that can be used are Visual Studio 6, MySql Server, Active Reports and other related components. It should be considered also that the components are flexible in mobile and PC application as possible.

4.2 System Design

System design is the process of defining the modules, activities, interfaces and data flow in a system. Figure 4 shows the system design diagram for ICT security policy.

From the diagram, System Managers have been identified as the most active users, who control and make sure every user enters the correct information into the system. In addition, IT managers also obtain the following information from the system, (a) details relating to the policies, (b) resource consumption, (c) document policy control activities and (d) user account.

Each user who wants to use the system needs to register for an account in the system. On the other hand, the management is more focused on data analysis and reports generated from the system. Users are able to generate a number of standard and also ad-hoc

reports. The ad-hoc reports are generated using existing software packages. All data contained in the system's database are seen as vital to its users. Each data is linked using a primary key field, that is, 'Policy Code' and 'User ID'.

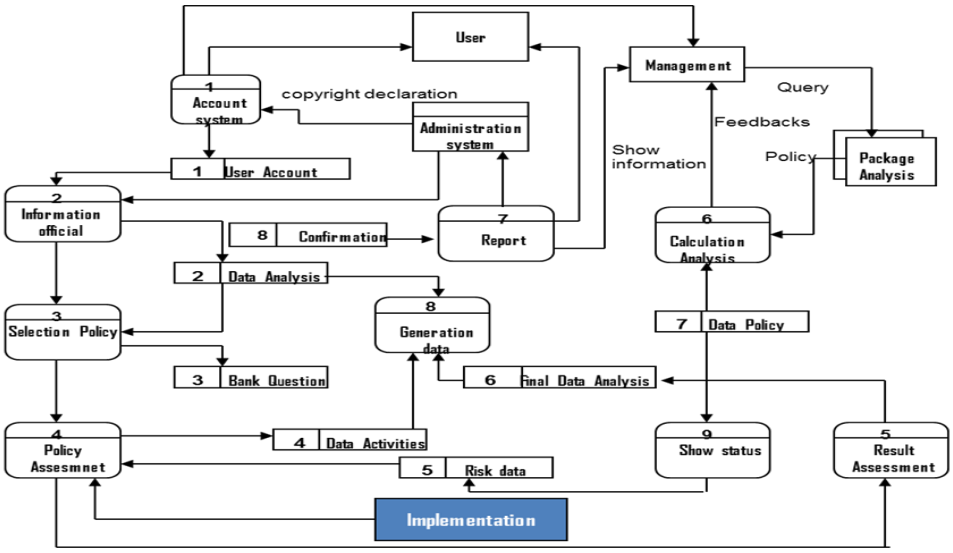

Figure 3: Design of ISPCS MDM

4.3 Project Development

In developing the system, different activities must be performed. Activities that can identify precise analysis and design of the project based on the status of the existing system. One of the common methodology is called System Development Life Cycle (SDLC) is suited in completing the system development. The SDLC describes activities and functions that all systems developers perform regardless of which approach they use. This methodology feature several phases as shown in figure 5 that marks the progress of the system analysis and design. The specific steps and sequences are needed to adapt and as required for the project, appropriate with management approaches.

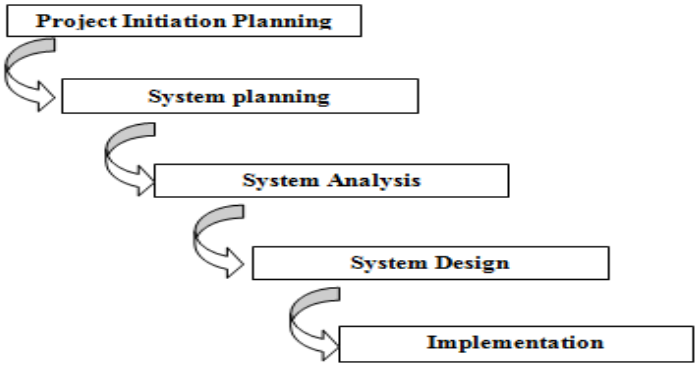

Figure 4: Project Development Life Cycle

4.4 Mobile Programming and Database Tools

Here are some mobile programming and database tools that we used in developing the system.

Android software. Android software development is the process by which new applications are created for the Android operating system. Applications are usually developed in the Java programming language using the Android Software Development Kit, but other development tools are available.

AppGyver. AppGyver makes a number of tools for mobile app development, including a PhoneGap extension called Steroids. Prototyper may be the most eye-opening, though, because it lets you glue together a few pages into a flexible prototype for testing your ideas. It will deploy the result to your device through a QR code or let you test the prototype on the AppGyver website.

Intel HTML5 Development Environment. Intel's HTML5 Development Environment is a cross-platform environment for developing, testing, and deploying applications on multiple device types. It is based on Web standards and was acquired by Intel when it purchased appMobi earlier this year. "It has a lot of really good strengths. It's a very goodtool," says Stephen Campbell, lead developer at Second Fiction game studio. Second Fiction has used the tool to build HTML5 and JavaScript apps. HTML5 and JavaScript code are wrapped in a container to run as a native app. "The primary thing about using HTML5 is it isn't as fast" as native code, he says. But work is being on this, he adds.

SQL Server. Database that can be connected to by a mobile computing device - such as smart phones or PDAs - over a mobile network, or a database which is actually carried by the mobile device. This could be a list of contacts, price information, distance travelled, or any other information. An example of this is a mobile workforce. In this scenario, a user would require access to update information from files in the home directories on a server or customer records from a database.

4.5 System Structure

The system is consists of the following hardware and software components, the Barcode/ QR Code enabled Smartphone and the ISPCS. This also includes other software and hardware requirements. Figure 9 shows the system components.

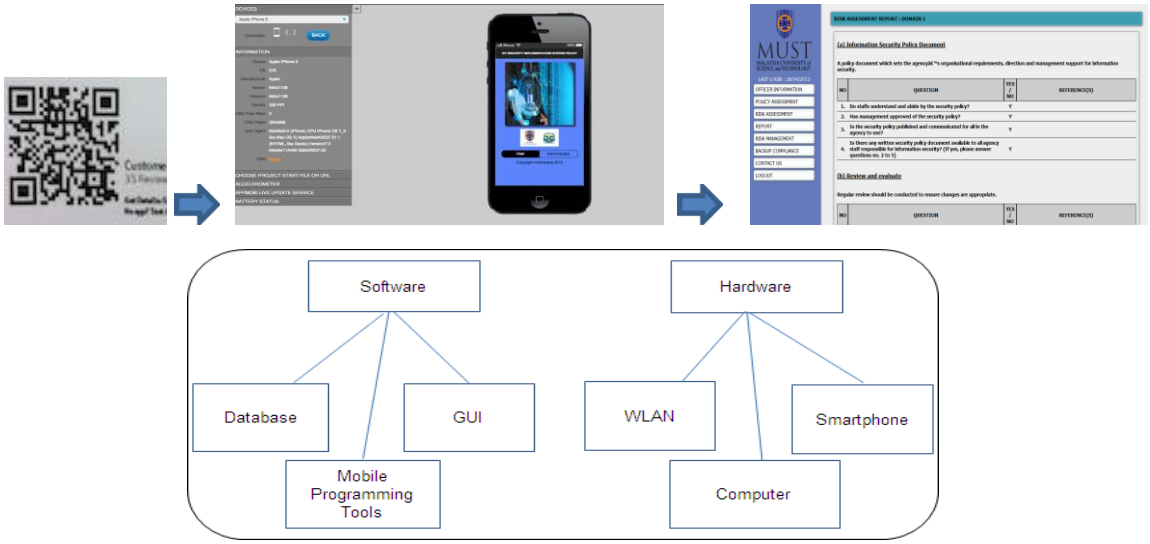

Figure 5: System Structure

5.0 IMPLEMENTATION

This chapter describes the implementation method for ICT Security Policy Compliance System (ISPCS). The system was tested using proper test procedures to ensure that it is built according to the requirements. The testing processes were conducted by MDC's ICT administrators.

5.1 General Modules

General modules are modules that are standard to all users, for example, login and logout screens. For the login screen, all users are required to enter their user ID and password as set up by the system administrator.

The same applies for the logout module, whereby users who have finished using the system are required to sign out from the system. The sign out will terminate the user's session, and reduce the risk for identity theft. A screenshot of the login main screen is shown below.

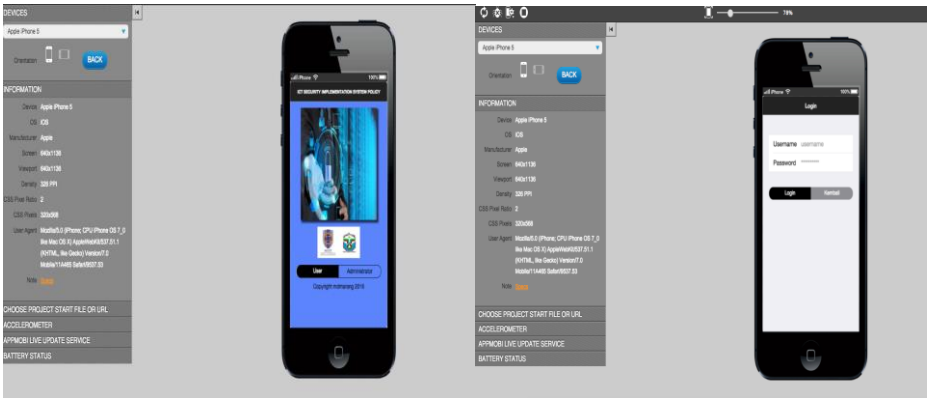

Figure 6: Login interface design

5.2 Users of the System

ISPCS has 5 categories of users, which are (a) system administrators, (b) managers, (c) policy implementers, (d) senior management or (e) stakeholders and normal users.

The modules in the systems were developed according to user's roles and activities. Furthermore, they were also based on the data and information access requirements. Generally, users want to be able to access the related policies for their departments or units as set by the BTM and MDC management. The appointed senior officers or officers will then perform an online assessment to check on the compliance of the ICT security policy. They will then use the reports to analyze the findings.

5.3 ICT Security Policy Compliance System (ISPCS) Modules

The modules in the system were developed according to the user requirements. These modules are based on the processes and activities undertaken by all levels of users. In addition, the activities are also controlled by the user roles. Generally, each user will perform similar activities, for example, entering and updating information, searching for information, selecting departmental policy, compliance assessment and subsequently, printing reports that have been processed. However, the information searched might vary depending on the users and their categories. In addition, each user has a different level of security access to the information.

The modules in the system can be categorized into general and specific and are implemented as described below.

Assess the Risk Level

The overall risk level for the Risk Assessment (RA) exercise conducted could be determined after the followingsteps were completed.

Identify the risk rating

(i) The owner or custodian of the information assets in the department shall answer a (□) at the close-ended "yes" or "no" questions.

(ii) All questions must be answered and not left blank. A blank answer will mean a default "no" answer.

Identify the risk level

After the task of identifying the safeguard rating, the risk level was obtained. The risk level result for each security domain is the addition of the additional safeguards as well as minimum safeguards to the risk rating obtained earlier for each security domain. (Risk Level = Risk Rating + Minimum Safeguards + Additional Safeguards Rating) (Refer Table 1: Risk Level Rating). This is the standardised (generic) table used to determine the risk level for each security domain.

Table 1: Overall risk rating matrix

Risk Likelihood	**Risk Impact**		
	Low (10)	**Moderate (50)**	**High (100)**
High (1.0)	**Low 10 x 1.0 = 10**	**Moderate 50 x 1.0 = 50**	**High 100 x 1.0 = 100**
Moderate (0.5)	**Low 10 x 0.5 = 5**	**Moderate 50 x 0.5 = 25**	**Moderate 100 x 0.5 = 50**
Low (0.1)	**Low 10 x 0.1 = 1**	**Low 50 x 0.1 = 5**	**Low 100 x 0.1 = 10**

Risk Scale: Low (1 to 10); Moderate (>10 to 50); High (>50 to 100)

6 .0 RESULT AND ANALYSIS

The proposed software was presented to the end users to determine its acceptability, functionality, reliability, efficiency, maintainability and portability of the system.

Rate	*Description*
5	Excellent
4	Very Good
3	Good
2	Fair
1	Poor

In terms of functionality the level of satisfaction in suitability, accuracy, interoperability, compliance and security was rated between Very Good to Excellent.

Table 2: Functionality

Criteria	Rate	Description
Suitability	4	Very Good
Accuracy	4	Very Good
Interoperability	4	Very Good
Compliance	4	Very Good
Security	5	Excellent

In terms of reliability, it includes the maturity and recoverability. As the user evaluated the system, the level of satisfaction is from Good to Very good.

Table 3: Efficiency

Criteria	Rate	Description
Time behavior	4	Very Good
Sources Behavior	4	Very Good

The maintainability of the system, after undergo testing the user evaluated the stability, analyzability, changeability between Good to Very Good.

6.1 ICT Security Policy Compliance Report

For each Security Domain assessment, the system will produce a report showing the percentage level of compliance. Figure 10 below shows the results of security domain compliance.

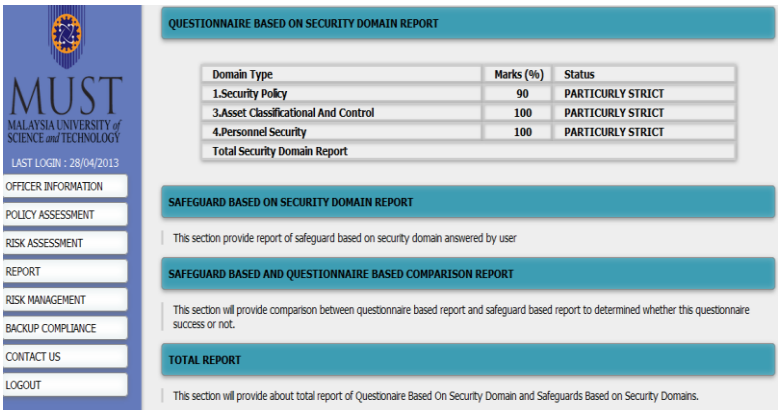

Figure 7: Security Domain Assessment in percentage

7.0 ACHIEVEMENTS

Some of the key success factors of the present study included fulfilling the project objectives and solving issues that emerged during the feasibility study. In addition, selecting the appropriate technologies, tools and techniques to support the analysis and development of the system also contributed to the success of this project. The database was designed systematically to ensure that it could support the needs of the data collection and analysis. A proper database design was essential for high-performance application. In addition, it also helped to ensure that ISPCS remained flexible and easy to manage and maintain.
Information is an asset to any organization and must be secured and protected. Moreover, the development of the system must ensure that the system is secure, confidentiality preserved and the integrity and availability of information are properly addressed. The interface must be easy to use and developed based on user requirements.

The software development process was also continuously improved based on the modules offered by the system.

7.1 Benefits of the System

The ISPCS was developed based on the feasibility study conducted on the organizations' business processes and issues faced in managing the policies. Among the benefits of the system are as follows:

1. Access and permission to the system are based on user groups where users are assigned to groups of ICT Administrator, IT Managers or normal users.
2. IT Administrator is capable to assign the permission in the system. In addition, IT administrator can also control the logins and is able to lock and unlock user access.
3. Information such as ISO 27001: 11 domains of Information Management and circulars from MAMPU were entered into the system.
4. The system is a mobile application; therefore, users are able to access the system from anywhere and anytime as long as they have the internet access. Mobile application has evolved significantly over recent years with improvement in security and technology, making it more reliable and highly deployable.
5. All information on policy activities are divided into four stages, (i) Preliminary, (ii) Planning, (iii) Implementation, and (iv) Proposal to ease the process of project monitoring.
6. Each stage is represented by percentage activities, selected or used from the overall domain, making it easier to monitor each stage of selected domain monitoring policy.
7. The standardization of the ICT security policy ensures that certain processes are performed consistently. In addition, by standardizing these policies, the monitoring process of other agencies will become easier.
8. The system also produced suitable reports tailored for management needs. For example, there is a list of selected policies, recommended policy as well as other ad-hoc reports generated from time to time.

8.0 CONCLUSION

In this paper a development of mobile ICT Security Policy Compliance System (ISPCS) application is presented. The development of the ISPCS in MDC has been important, as it has been in any other organization in this country. The system provides a strategic framework and defines common rules to be followed by everyone within MDC. The development of the software policy covers four important activities, namely management policy, evaluation policy, process governance policy and compliance improvement policy
Evidently, the ICT Security Policy system has been developed to improve the services offered by Information Technology Division (BTM). We believed that ISPCS application uses software components that are being re-used repeatedly; hence, component re-used for mass application developments is necessary. We design a mobile ISPCS as our sample application.

The ISPCS was developed to address business issues and problems faced by users. Furthermore, it was also meant to motivate the ICT Administrator to share his knowledge with related users and stakeholders in order to improve the rules and policy of computer usage in MDC. We also believe that by implementing ISPCS, our organization will have continuous protection and privacy for our information and ICT assets.

In conclusion, the proposed ISPCS has fulfilled the objectives of the study which includes increasing the efficiency of the current information management system. Finally, it is recommended that the study could be expanded further as discussed earlier in order to realize the full potential of the system on offer and bring many benefits to the organization

ACKNOWLEDGEMENTS

Acknowledgement thanks to Marang District Council who provided funding for this research.

REFERENCES

[1] Android Developers website. https://developer.android.com/.
[2] Android o_cial website. http://www.android.com/.
[3] Ali Salman, 2010, "ICT, the New Media (Internet) and Development: Malaysia Experience" The Innovation Journal: The Public Sector Innovation Journal, Volume 15(1), article 5.
[4] Bahrami, A., 1999 "Object-oriented Systems Development: Using the Unified Modeling Language", McGraw-Hill Inc., Singapore.
[5] Boston B, Greenspan, 2004 J, Wall, D, MySQLPHP Database Applications 2nd Ed, Wiley Publishing, Inc., Indianapolis.
[6] British Standards Institution (BSI), 2002 Information Security Management Systems.
[7] ISO/IEC TR 13335-1:1996, 1996, GMITS -Concepts and models for IT Security.
[8] ISO/IEC TR 13335-2:1997, 1997, GMITS -Managing and planning IT Security.
[9] ISO/IEC TR 13335-3:1998, 1998, GMITS -Techniques for the management of IT Security.
[10] ISO/IEC TR 13335-4:2000, 2000, GMITS -Selection of safeguards.
[11] ISOIlEC FDIS 27001:2005, 2005, Information Technology -Secutity.
[12] ISO/IEC FDIS 17799:2005, 2005, Information Technology - security management systems – Requirements.
[13] ISMS and A LevellCT Through Diagrams, 2010, NISER.
[14] IT Security Promotion Committee Japan, Julai, 2009 GUidelines/or IT Security.
[15] MAMPU, 2002, The Malaysian Public Sector Management of Information Security.
[16] Information Technology Instructions, December 2007.
[17] MAMPU, 2002, Techniques-Information security management systems – Requirements.
[18] MDC, 2009, ICT Security Policy Version 2.
[19] MAMPU, Julai, 2009, ICT Security Policy Version 5.3.
[20] New Jersey, 2002 Digital Crime and Forensic Science in Cyberspace, Prentice-Hall, Englewood Cliffs.