Information Security Risk Management in Malaysian Remote Sensing Agency (MRSA).

Introduction

This project will investigate whether current information security risk management policy in MRSA is adequate or recommendations for improvement should be proposed. Risks are those events with the potential to have a significant negative impact on the organisation (Hopkin, 2013). Information technology and communication (ICT) has evolved and changed many ways of how typical operations being simplified and reduced in terms of time and costs. The expanding usage of ICT, especially through borderless information via internet exposes government information to the risk of intrusion and leakage.

IT risks can be classified into three categories (I) technical or operational; (II) data and information security; and (III) organisation, project, legal and human or people sides (Ahlan and Arshad, 2012). This project will focus on the second category, information security risk management implementation in MRSA. Information security risks are events which can potentially cause significant negative impact on the confidentiality, integrity or availability of the organisation strategic information. Thus, it is crucial that information security risks are managed properly to ensure all predicted consequences and outcomes are responded appropriately to minimise the impact.

Background

Malaysian Remote Sensing Agency (MRSA), a department under the Ministry of Science, Technology and Innovation Malaysia was established in 1988 to spearhead the development and operationalisation of remote sensing, geographical information system (GIS) and related technologies in Malaysia. Realising the importance and criticality of the information handled by the department, an initiative has been undertaken to adhere to best practices in information security.

In 2003, the department was involved in the government pilot project with SIRIM QAS International to adapt to the standard set in BS ISO/IEC 17799:2000 ‘Information Technology - Code of practice for information security management’ which was then revised in 2005 and renamed as BS ISO/IEC 27001:2005 ‘Information System Management Standard’ (ISMS). Three years later, MRSA obtained the certification and became the first government department in Malaysia to be certified with ISMS for their core business, data services scope. Continuous improvements have been implemented throughout the years ever since.

Aims and Objectives

The aims of this project are to study current implementation of information security risk management in MRSA, to find any gaps or weaknesses and to suggest improvements. In order to achieve the goals, these objectives have been set for this study:-

1) To measure the effectiveness of current policies.
2) To measure the maturity of the information security risk management.
3) To compare the model used for information security risk management in Malaysia and other countries.
4) To find the gaps and weaknesses.
5) To propose improvements and enhancements.

Problem Statements

Even though the policies and procedures are reviewed every year to cater for organisational changes and restructuring, there has been no effort in measuring the effectiveness of the policies. Audits only discover the non-conformity to the policies and procedures set by the standard without taking into consideration their appropriateness and efficiency. **How effective are current policies in managing information security risks? Are there any gaps or weaknesses? What can be done to improve it?**

2015 marked the 10th year of ISMS certification in MRSA. Therefore, it is high time to measure the maturity of its information security risk management. Since MRSA was the pioneer in adapting international information security management standard in Malaysian public sector, it could be a perfect case study to resemble the maturity as a whole. **How mature is the information security risk management after 10 years of following the standard?**

The British Standard Institution (BSI) has published a revision to the BS ISO/IEC 27001:2005, named BS ISO/IEC 27001:2013 with major changes to risk assessment requirements to align with BS ISO 31000:2009 'Risk Management – Principles and guidelines'. Currently, risks assessment in MRSA is done manually using Microsoft Excel on the assets included in the scope. This needs to be revised and new risk assessment methodology needs to be formularised to cater for the new requirements. According to the new standard, risk management takes human and cultural factors into account. **Are the principles and guidelines stated in the documents suitable for Malaysian social and cultural, political, legal, regulatory, financial, technological and economic factors?**

Proposed Methodology

This study is proposed to be empirical in nature where data will be collected through observation, documents reviews and interviews. Internal documents such as risk management policy, risk assessment method, audit reports and related procedures will be reviewed to analyse current implementation of information security risk management in MRSA. Malaysian government circulars and related BSI standards documentation will also be crossed check with current execution.

Interviews with risk coordinators will be conducted to investigate about current scenario and unveil any problems faced in managing information security risk in MRSA. To find the view from the perspective of the stakeholder, an interview with the Director of Data Services Department will be conducted. Finally, an interview with the Director of ICT who is responsible in the department information security as a whole will be conducted to learn about his experience in managing information security risks in MRSA.

The author is an IT officer in MRSA currently on study leave and has access to internal data and documentations required for this study. For comparison with practices in other countries, the models used in the United States General Accounting Office, the New South Wales Department of Education and Communities and the United Kingdom Government Actuary's Department which are published online will be evaluated against MRSA current policies.

Expected Deliverables

The outcome of this study is a dissertation about the information security risk management in a Malaysian government department which has adapted to international standards for more than a decade. Current policies will be analysed and compared to the ones used by others. Finally, improvements will be suggested to minimise the gaps and further enhance their procedures. Proposed recommendations which are accepted by the stakeholders will be implemented when the author come back to Malaysia to continue her work after completing her postgraduate study.

Evaluations

Two types of evaluations will be carried out in this study namely user evaluation and self-evaluation. In user evaluation, suggested improvements and enhancements from the study will be submitted to the stakeholders for evaluation and feedback. If they agree with the recommendation, it can be forwarded to the management committee for endorsement. Otherwise, their valued views, comments and feedbacks will be analysed for further discussions. In self-evaluation, the outcome will be compared to initial objectives to examine whether the aims of this study are achieved.

Project Plan

The Gantt chart in **Appendix 1** explains proposed time plan for this project.

References

Ahlan, A. R. and Arshad, Y. (2012) *Understanding Components of IT risks and Enterprise Risk Management: A Literature Review in Risk Management*. InTech Open Access Publisher.

BS ISO/IEC 27001:2005 (2005) *Information System Management*. British Standard Institute.

BS ISO 31000:2009 (2009) *Risk Management – Principles and guidelines*. British Standard Institute.

Hopkin, P. (2013) *Risk Management*. Kogan Page Limited.

Malaysian Remote Sensing Agency Portal: http://www.remotesensing.gov.my accessed on 10th March 2015.

New South Wales Department of Education and Communities Risk Management documentation: https://www.det.nsw.edu.au/policies/general_man/erm/PD20040036.shtml accessed on 10th March 2015.

United States General Accounting Office Risk Management documentation: http://www.gao.gov/special.pubs/ai00033.pdf accessed on 10th March 2015.

United Kingdom Government Actuary's Department Risk Management documentation: https://www.gov.uk/government/publications/strategic-risk-management accessed on 10th March 2015.

Appendix 1 – Proposed Time Plan

		Feb				Mar				Apr				May				Jun				Jul				Aug				Sep			
Conceptual Study		▩	▩	▩	▩	▩	▩	▩	▩																								
1.	Theoretical background and concepts	🟦	🟦	🟦	🟦																												
2.	Literature review		🟦	🟦	🟦	🟦	🟦	🟦	🟦																								
3.	Policies, standards, guidelines		🟦	🟦	🟦	🟦	🟦	🟦	🟦																								
4.	Initial report			🟧	🟧	🟧	🟧																										
5.	Interview questions design							🟦	🟦																								
Empirical Study								▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩															
1.	Review of related documents and stds.									🟦	🟦	🟦	🟦																				
2.	Data collection - interview									🟦	🟦	🟦	🟦																				
3.	Data processing											🟦	🟦	🟦	🟦																		
4.	Data analysis														🟦	🟦	🟦	🟦															
5.	Progress report							🟧	🟧	🟧	🟧	🟧	🟧	🟧																			
Measurements																	▩	▩	▩	▩													
1.	Information security risk maturity																🟦	🟦															
2.	Information security policy effectiveness																		🟦	🟦													
Results															▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩	▩		
1.	Findings																				🟦	🟦	🟦										
2.	Evaluations - proposal submission																							🟦									
3.	Evaluations - feedback from stakeholders																								🟦	🟦	🟦	🟦					
4.	Discussions																								🟦	🟦	🟦	🟦					
5.	Conclusions																											🟦	🟦				
6.	Final dissertation														🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧		

Deadlines:-
Initial report – 12 March 2015
Progress report – 8 May 2015
Dissertation – 11 September 2015