ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations

Shamsuddin Abdul Jalil and Rafidah Abdul Hamid

Abstract: *Since March 2003, the Information Security Management Systems (ISMS) Pilot Program has been jointly conducted by National ICT Security & Emergency Response Centre (NISER) and SIRIM QAS International Sdn. Bhd. which is a wholly owned subsidiary of SIRIM Berhad. The certification offered by SIRIM QAS is based on the British Standards Institute's (BSI) BS 7799-2:2002 standard. It is intended for this paper to discuss the outlined benefits of the ISMS pilot program and the ISMS itself, the challenges faced during the ISMS implementation phase and recommend suggestions to improve the overall quality of the ISMS implementation process in organizations.*

Keywords*: ISMS, pilot program, benefits, challenges, recommendations*

I. INTRODUCTION

The progress of data protection standards implementation in Malaysia is slowly gathering pace and its importance is becoming more and more apparent to organisations around the country.

This is the view held by NISER (National ICT Security and Emergency Response Center) which is currently staging an audit on data protection methods in local organisations since March 2003. The audit came at the heels of a pilot project called the Information Security Management Systems (ISMS) that NISER jointly conducted with SIRIM QAS International Sdn. Bhd.. Initially 10 organisations have participated in the pilot programme. NISER's role in this programme is to provide technical assistance in ICT Security to SIRIM QAS in terms of the development of the programme as well as providing training and auditing services.

The BS7799-2:2002 standard has been adopted in the pilot programme for certification purposes. The BS7799-2:2002 is the de-facto standard for data protection and is well accepted in international communities and thus was the standard chosen for the ISMS pilot programme.

Based on the experience gathered from the ISMS implementation and audit processes, the authors feel that they are in a good position to be able to discuss the various

benefits and challenges faced by organisations during ISMS implementation. The authors will also provide some recommendations to smoothen the ISMS implementation process.

II. BRIEF ISMS HISTORY AND BACKGROUND

ISMS was initially the initiative from the UK Department of Trade and Industry in 1995 and its main objective was to provide a code of practice to information security practitioners. ISMS concerns itself with the security of information whether in physical or logical form and focuses on three areas: the confidentiality, integrity and availability of information or usually referred to as CIA. ISMS is made up of two parts: part 1 which is known as ISO/IEC 17799:2000 which is the code of practice for information security management and part 2 which is known as BS7799-2:2002 which provides specifications with guidance for use for ISMS implementation.

Part 1 lists out the recommended 127 controls or safeguards (not all is to be implemented, this is to be decided based on the risk assessment process) in detail and it provides detailed guideline on how the controls are to be implemented. The part 2 focuses more on the proper techniques of implementing ISMS where it makes it compulsory to conduct certain practices such as conducting a comprehensive and systematic risk assessment and having a risk management framework in place, having proper documentation management process and control of records, setting up a security forum and others. ISMS implementation needs to follow the PDCA (Plan - Do - Check - Act) model as depicted in the diagram below for an effective and comprehensive implementation.

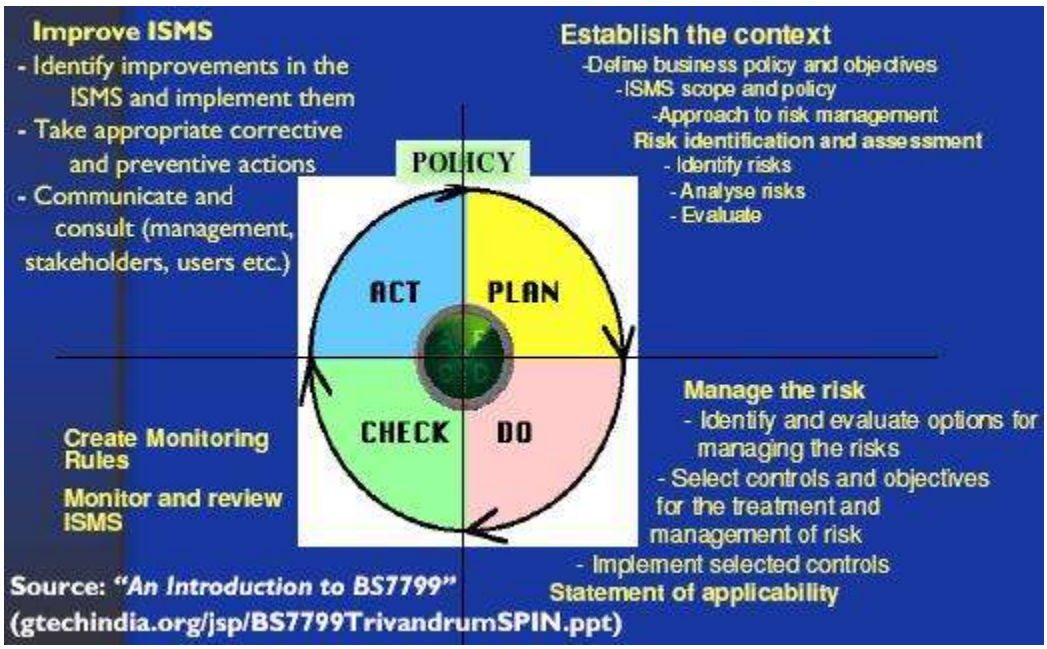

Diagram 1: PDCA Model

III. WHY THE NEED FOR ISMS IMPLEMENTATION IN MALAYSIAN ORGANISATIONS?

The rising number of security breaches over the years have contributed to increasing security concerns among organisations throughout the world. In Malaysia specifically, the number of security breaches have continued to increase over the years and the breaches comes in different types and forms. The following diagram obtained from NISER's ISMS Survery in 2003 shows the different types of security breach suffered by various organisations in Malaysia.

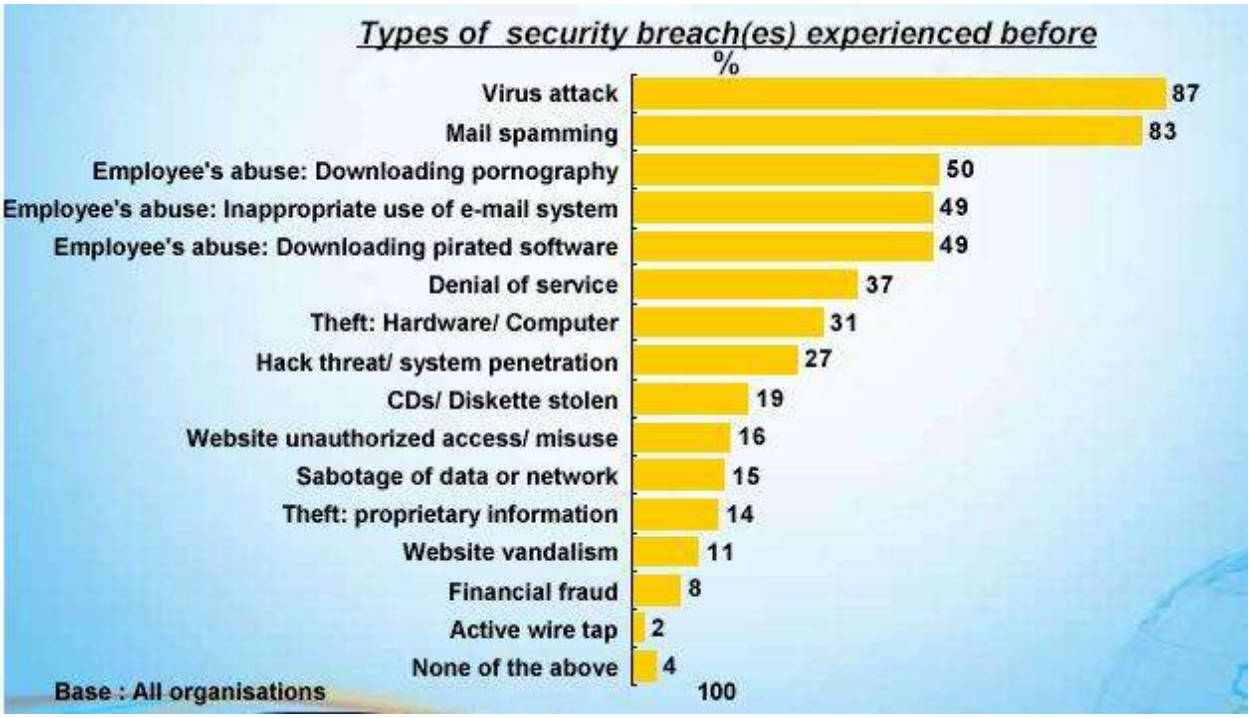

Diagram 2: Types of Security Breach(es) Experienced before

Therefore there is a more urgent need than ever to look at security from a holistic perspective, and to have a security management methodology to protect vital information systematically.

Thus it is expected that the ISMS Pilot Program will lead the way for more ISMS implementations in the country. The various benefits associated with implementing ISMS will be discussed in one of the following sections in the paper but overall, the pilot program is expected to benefit the participating organisations tremendously in terms of improving their information security setup and ensure data security and

ultimately it is expected that other organisations will follow suit and undergo a similar process to better protect themselves from information security breaches.

IV. WHO ARE SUPPOSED TO IMPLEMENT ISMS?

There are no exceptions when it comes to which organisations that are supposed to implement ISMS. Basically every organisation that handles information are recommended to implement it, be it financial institutions, government agencies, IT companies, hospitals, universities, insurance companies, R&D-based companies and so many others.

V. EXPECTATIONS WITH ISMS IMPLEMENTATION

ISMS is a relatively huge project, although the scale on which it is implemented also depends on the scope selected for implementation. Thus with such a project, especially one that is as comprehensive and requires various resources to be used to ensure its success, the level of expectations of its success are also high. Some of the most common expectations[3] that were anticipated by organisations that implement ISMS in the pilot programme as observed by NISER include:

A. Risks and losses will be minimised

With an effective and comprehensive ISMS implementation, the number of security breaches suffered by organisations can be reduced. Thus any security risks and losses will subsequently be minimised. This is normally the least expected return of an ISMS implementation and should be the main objective of such an exhaustive project undertaken by any organisation.

B. Compliance to rules, legislation, company standards and practices

By implementing ISMS, organisations will also be automatically be compliant to any relevant rules, legislation, company standards and practices. This is so because there is a specific clause in ISMS that mandates organisations to be compliant to them to improve corporate governance and to avoid being held liable for certain legal issues.

C. Improved safety

Obviously, by implementing ISMS which focuses on securing vital company information

from being misused by unwanted intruders, the overall safety of information, personnel and assets are being assured. Thus by performing the risk assessment process and implementing the identified controls to mitigate the risks as warranted by the ISMS, it will help to prevent unwanted security breaches from happening and even in the event that something does happen, organisations will be well prepared for it by the implementation of incident response handling procedures and business continuity management.

D. Reliable operations

By implementing ISMS, organisations can be more assured regarding the reliability of its operations as any weak points to it should already been identified and mitigated appropriately. Thus, it will enable organisations to plan ahead of a crisis or disaster and develop appropriate recovery procedures to ensure downtime of operations are minimised.

E. Business continuity

As explained in the points C) and D) above, since Business Continuity Management (BCM) is one of the domains in ISMS, it will therefore benefit organisations tremendously from ISMS implementation as with proper BCM implementation, the overall downtime for business operations that may be caused by realization of threats such as flood, fire, theft and others can be minimised. Thus it will ensure that the business continues to operate in the event of a crisis or disaster, although most possibly not at 100% as during normal operations, although this depends on the chosen recovery strategy.

VI. ISMS BENEFITS

There are various benefits associated with a comprehensive ISMS implementation [3]. The following diagram highlights some of the benefits of ISMS as listed out by the participants of NISER's ISMS Survey.

Diagram 3: ISMS Advantages

The following are some of the benefits associated with ISMS implementation that we observed during the running of the pilot programme in participating organisations.

A. Improved understanding of business aspects

Most of the organisations agree the notion that their understanding on their business process functions and resource requirements have increased with ISMS implementation. This is because in ISMS, there is a need for a detailed study on the business processes in organisations to determine the assets involved and the different types of risks associated with the assets. This is highly beneficial as not only the organisation will have a deeper understanding on its business processes, but it will also enable them identify the exact number of assets needed to run the business processes and thus make the necessary adjustments to improve its performance.

B. Reductions in security breaches and/or claims

A proper and comprehensive ISMS implementation can significantly reduce the number of security breaches and/or claims in organisations. This is one of the major selling points of implementing ISMS and organisations that are serious in attempting to put a stop to unwanted and costly security breaches are encouraged to take a deep look in taking up the option.

C. Reductions in adverse publicity

A successful ISMS implementation will assist to put stop to malicious rumours regarding the state of organisational security. The pilot program participants agree that with a comprehensive ISMS implementation, they are much more able to defend the organisations' integrity from being compromised by ill-intended parties.

D. Improved insurance liability rating

By demonstrating that there are sufficient controls to prevent against security breaches against critical information, ISMS have managed to assist organisations in improving their insurance liability ratings

E. Identify critical assets via the Business Risk Assessment

Risk assessment is one of the major components in ISMS because through this process, not only that all the assets in the organisation will be identified, the different types of threat, vulnerability and risk to those assets will also be determined and thus appropriate controls can be implemented to mitigate those risks. All the participating organisations agree that risk assessment is very beneficial to them and have assisted them in securing their organisations better.

F. Ensure that ”knowledge capital” will be ”stored” in a business management system

Since one of the focus of ISMS is on the concept of availability, it encourages organisations to develop a knowledge database where they would be able to tap on the needed expertise in situations where certain personnel or system are deemed to be unavailable.

G. Be a confidence factor internally as well as externally

Not only employees will feel more confident in performing their assigned tasks in a secure business environment, third parties including clients and service providers will also feel more secure doing work with an organisation that places extra emphasis on securing information. We noted that this is so, especially in the organisations that have managed to successfully implement ISMS either for compliance and/or certification purposes.

H. Systematic approach

ISMS provides a systematic way for organisations to manage their information security setup through the implementation of the PDCA model that it adopts. The pilot programme participants agree that ISMS enables them to manage and secure their information effectively as well as systematically.

I. Provide a structure for continuous improvement

With the use of the PDCA model, ISMS will ensure that the framework to enable organisations to continously improve their information security management setup is in place. Again, this view is shared unanimously by all the participating organisations.

J. Enhance the knowledge and importance of security-related issues at the management level

ISMS requires the management team's participation in the entire ISMS process cycle and thus it will automatically enhance their awareness and knowledge on the importance of security-related issues in the organisations. The participants agree that with awareness and much more involvement on the ISMS project at the management level, they are able to implement ISMS more effectively.

VII. ISMS CHALLENGES

There are various challenges that awaits ISMS implementors[3]. Among them that NISER have observed during the pilot programme implementation are:

A. Fear / Resistance to change

By implementing such an extensive management system in the workplace, changes are definitely going to be made, either in the working process, alterations in personnel responsibilities and many other areas. We observed that some organisations are quite recluctant to make major changes without elaborate justifications in place as it will impact the operations of their business.

B. Increased cost

By implementing ISMS, either directly or indirectly, it will definitely cause an increase in

the costs incurred especially when implementing the controls identified to mitigate the known risks. We discovered that some of the organisations simply did not have adequate budget to allocate the funds and/or resources to implement such a system.

C. Inadequate knowledge as to approach

Many organisations still do not have the know-how on proper ISMS implementation and they may not have personnel who are qualified subject matter experts in the area. Thus this may lead to the delay or avoidance on the implementation.

D. Seemingly huge task

Depending on the scope, ISMS can sometimes be such a huge task to complete. Besides the extensive documentations that are required to be prepared, the other activities that needs to be done such as managing resources, user training and awareness and many others may prove to be too daunting to be completed by some of the participating organisations.

VIII. ISMS RECOMMENDATIONS

To ensure a better and effective ISMS implementation, it is recommended that the following guidelines are followed to improve the process:

A. Critical Success Factors

Organisations are encouraged to take into account the Critical Success Factors (CSFs) listed out in the ISO/IEC 17799:2000 standard (*Please refer to page xi in the standard for more details*) to ensure implementation success. Organisations need to place extra importance on the listed factors and attend to them appropriately to ensure that the ISMS implementation process runs smoothly.

B. Complete PDCA Cycle

Ensure that during the ISMS implementation process, organisations adhere to the requirements stated in the Plan-Do-Check-Act (PDCA) model and complete all the activities mentioned in the PDCA cycle accurately and comprehensively.

C. Refer to both the BS7799-2:2002 and ISO/IEC 17799:2000 standard during implementation

Some organisations tend to focus more on the BS7799-2:2002 standard when implementing ISMS and ignore the detailed control guidelines provided in the ISO/IEC 17799:2000 standard. Therefore by doing so they are unable to implement the identified controls properly and this in turn leads to many mis-interpretations regarding the control requirements and failures in implementing them.

D. Avoid the common shortcomings in ISMS implementation

To ensure a smoother ISMS implementation, the most common shortcomings as observed by NISER in the pilot program needs to be avoided. For further details, please refer to the paper entitled: *"Common Shortcomings in ISMS Implementation"* written by Shamsuddin Abdul Jalil (e-mail: ssuddin@niser.org.my), Rafidah Abdul Hamid (e-mail: rafidah@niser.org.my) and Ariffuddin Aizuddin (e-mail: ariff@niser.org.my). Please contact the authors for a copy of the paper if interested.

IX. CONCLUSION

In summary, it is hard to ignore the fact that all the parties involved in the running of the ISMS pilot programme have benefited tremendously from it. Not only the participating organisations have learnt a valuable methodology to secure and manage their information systematically, but they have managed to form a forum to discuss the issues and problems they are facing with ISMS implementation. The programme coordinators, consultants, trainers and auditors have gained valuable experience as well. It is hoped and anticipated that in the near future more and more organisations in Malaysia, especially those from the government and financial sectors will view ISMS as a necessity for them in order to assist them to grow their operations and business and secure the vital information and assets that enables them to do so.

REFERENCES

[1] "History of 7799"
Available at http://www.gammassl.co.uk/bs7799/history.html

[2] "An Introduction to BS7799"
Available at http://gtechindia.org/jsp/BS7799TrivandrumSPIN.ppt

[3] Inger Nordin, "Implementation of an ISMS - A process approach", Feb 2003.
Available at http://www.ivpk.lt/dokumentai/prezentacijos/09%20Information%20Security20Management%20System%20-%20Implementatio.ppt

[4] Inger Nordin, "Information Security Management System (ISMS) – Introduction", Feb 2003. Available at http://www.ivpk.lt/dokumentai/prezentacijos/08%20Information%20Security%20Management%20System%20-%20Introduction.ppt