Risk Identification for an Information Security Management System Implementation

Nor Aza Ramli, Normaziah Abdul Aziz
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia
Gombak, Malaysia
azaramli@gmail.com, naa@iium.edu.my

***Abstract* — ISO/IEC 27001 is an international standard that provides a set of requirements for an Information Security Management System (ISMS) implementation. A risk assessment exercise for an ISMS implementation requires human expertise with comprehensive understanding and considerable knowledge in information security. A common risk assessment exercise is based on three sub-processes, namely, risk identification, risk analysis and risk evaluation. The lack of tools especially in the automation of risk identification emphasized the need of experienced personnel and this becomes a challenge for organizations seeking compliance with the ISMS standard. This paper proposes a relationship concept in asset and threat identification which is part of the risk identification sub-process. The concept provides a foundation to automate the risk assessment process for an identified scope of an ISMS implementation.**

Keywords – ISMS; information security risk; asset identification; threat; risk assessment

I. INTRODUCTION

A. Information security

Information is an asset that has value to an organization. It is, like other important business assets, essential to an organization's business and consequently needs to be suitably protected, which is especially important in the increasingly interconnected business environment [1]. The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) published various standards for ISMS. ISO/IEC 27002 defined information security as the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [1]. In order to achieve information security, an organization needs to first identify what are the assets that need the protection and perform a risk assessment exercise to determine the level of risks and the suitable set of controls to minimize these risks, eventually securing the assets.

B. Information security risk

Organizations that are dependent on information technologies consequently have to face a common issue of managing information security risks which are inherited with the use of the technologies. In 2009, SANS Institute has issued a report entitled "The Top Cyber Security Risks" that discussed on the importance of understanding security threats and their corresponding vulnerabilities prior to identifying security controls to mitigate the associated risks [2]. Global State of Information Security Survey, 2010 has in its findings, organizations have considered taking a risk-based approach as well as adopting a recognized security framework in addressing information security issues [3]. According to Humphreys, if an organization does not know the risks it faces, it will not be able to implement proper and effective protection [4]. In 1995, Kailay and Jarrat have highlighted that one of the gaps then was the limited risk analysis methodologies and corresponding tools for certain domain users [5]. At present, that gap has been addressed through publication of documented guidelines on several risk assessment methodologies such as the ISO/IEC 27005:2011 [9]. However, methodologies alone could not guarantee an effective information security risk assessment. Risk assessment process comprises of three sub-processes, namely, risk identification, risk analysis, and risk evaluation. Automation of the process is common in many risk assessment tools with the exception of risk identification. Hence, automation of risk identification would be useful for organizations especially for those carrying out risk assessment for the first time.

C. Information Security Management System (ISMS)

Acknowledging the importance of understanding and managing information security risk, a global effort by information security practitioners has resulted in the development of a standard for an Information Security Management System (ISMS). ISMS standards started in the early 90s with the first draft of an information security management standard published as British Standard (BS), BS 7799. It focused on security related to people, processes, information as well as information technology [4]. In 2005, BS 7799 Part 2 became an international standard known as ISO/IEC 27001:2005 [6]. ISO/IEC 27001 standard is a specification for information security management system developed jointly by the ISO/IEC, and was published in 2005 [7]. This standard adopts a risk-based approach for an effective information security management taking into consideration the information security aspects of various areas within an organization [6]. In an ISMS implementation, organization will have to identify a scope for the ISMS and this scope will be subject to a risk assessment to identify appropriate controls to mitigate the identified risks.

Current tools including documented guidelines in risk management such as the ISO/IEC 27005:2011 could be used by

 ISBN: 978-1-61208-209-7

organizations to facilitate the risk assessment process [9]. However, these tools are lacking in automation and its usage requires human expertise with professional judgment and knowledge of information technologies as well as capability to relate information security threats with organizational risk management [5], [8], [10], [12].

The lack of tools especially in the automation of risk identification emphasized the need of experienced personnel and this becomes a challenge for organizations in implementing information security management especially those seeking compliance with the ISMS standard.

This paper discusses some relationship concepts in asset and threats identification. Identifying accurate assets and relevant threats are very important to ensure reliable risk assessment results. This is part of our current work to automate the risk assessment process.

The contribution in this paper is the identification of assets and their relationships to relative threats for an ISMS scope to facilitate automation of the risk assessment process. The relationships developed in this study are limited to the identified ISMS scope which is secure data centre. It aims to address automation in risk assessment for network security threats which can be expanded to other category of threats.

II. RELATED WORK

Previous works on similar efforts to automate risk assessment process are reviewed in this section. In 1995, a prototype expert system for computer security risk analysis and management was developed at the School of Computer Science, University of Birmingham. RaMEX was developed based on RAM (Risk Analysis and Management) methodology and concentrated on the category of intentional threats [5]. As the name suggests, RaMEX facilitates risk assessment step-by-step following a methodology developed specific for it.

Another work sighted has emphasized on the importance of using previously acquired knowledge in risk analysis. A risk analysis system in electronic commerce environment was developed at the Korea Advanced Institute of Science and Technology, Seoul [10]. The system was based on case-based reasoning (CBR), taking advantage of the experience and learning from incidents knowledge into the analysis of risks. According to Liao and Song [11], even though the CBR approach could make use of past solutions, it takes time to collect such cases and in the event that a case is the first one to occur, the results of the assessment could be limited.

Liao and Song have taken a different approach in developing a computer-aided system to facilitate risk assessment process [11]. Their work has focused on transaction-based risk assessment by looking at the value of a transaction to an organization to determine the impact of losses to the business. Instead of depending on past solutions, risk assessment is performed based on transactions that have been defined and known to the system [11].

Similarly, a work by Aime, et al. [8] approached risk analysis based on models that can be built at runtime and during system monitoring of a known target system. The model was used to automate some portion of the risk analysis processes namely the collection of threats data, the identification of applicable threats to the target system and the calculation of risk level.

In 2007, Software Engineering Institute at Carnegie Mellon University has published a technical report on OCTAVE Allegro which focused on information assets in its methodology that is used for identifying and evaluating information security risks. It approached risk assessment by focusing on information asset and its containers such as people, physical and technology aiming to produce a more robust assessment result [12]. In 2009, Chivers et al. has assessed risks to a particular system incrementally using formally defined risk profiles [13].

As a summary, scholars have carried out studies applying different approaches on various scope of assessment to achieve improvements in risk assessment process including targeting its automation.

III. OUR PROPOSAL

The core idea of this research is to automate all the three sub-processes in a risk assessment process for an identified scope of ISMS. We are proposing to focus on the risk identification as this is a sub-process where domain knowledge in information security needs to be applied. Domain knowledge on what are the significant assets for an identified ISMS scope, and what are the threats and corresponding vulnerabilities on those assets, will be modelled using an ontology editor to develop relationships of these important risk assessment parameters. With our proposed work, the tools are expected to be easily comprehended by a non-experienced risk analyst as both angles of the risk assessment i.e. the methodology and information security domain knowledge would have been carefully modelled with the use of ontology rules. Involvement of an experience risk analyst could be minimized and their resources could then be utilized effectively, only when needed.

There are various tools for ISMS implementation that addressed the whole process of the management system based on the “Plan-Do-Check-Act” (PDCA) model. The tools have been designed to ensure implementation complies with the standard, i.e., ISO/IEC 27001:2005. As ISMS adopts a risk-based approach, risk assessment is one of the main components of these tools. As far as automation is concerned, current tools have been observed to facilitate the end-to-end risk assessment methodology as well as performed calculation based on selected formulas during risk analysis and risk evaluation sub-processes exercises. Automation of the risk identification sub-process, however, has not been included as part of the tools’ feature. Considerable involvement of a competent risk analyst with information security domain knowledge was still required. For example, to identify assets of an ISMS scope given the possible list of asset types which is taken from guidelines such as the ISO/IEC 27005 is rather confusing. Is an identified asset subject to risk assessment or the asset is in fact a control that has been implemented to mitigate a risk? As an example, is a firewall an asset that needs to be protected or is it a control that has been implemented to protect an asset? Forming the basis of what assets are indeed subject to risk assessment for a specified

 ISBN: 978-1-61208-209-7

ISMS scope have yet seen to be explicitly addressed by existing tools. In a common risk assessment exercise, expert resources have been observed to be utilized ineffectively due to this lack of automation. The output of this study is to build a prototype that enables risk assessment automation for organizations going for ISO/IEC 27001 certification. The proposed relationship concepts in asset identification contributed to the automation of the risk assessment for an identified scope of implementation. Protégé OWL (Web Ontology Language) was used to create classes and corresponding rules to demonstrate the relationships. Protégé is an ontology editor which is based on an open-source platform. It was developed by Stanford Center for Biomedical Informatics Research at the Stanford University School of Medicine. There are two types of the system; Protégé Frames and Protégé Owl. The former supports frame-based ontology while the latter supports Web Ontology Language. Both are actively being used as well as updated from time to time as observed from its website [14].

A. ISMS Scope

According to the International Register of ISMS Certificates, there were 7,686 certificates registered by organizations from eighty-five countries [15]. Malaysia held fifty-eight certificates and was ranked at 14th place as of March 2012. About eighty percent of the certificates in Malaysia have identified scope that is related to secure data centre service. Implementation of ISMS to manage a secure data centre is thus indicated to be very relevant in the context of organizations that highly depending on IT as their business enabler.

B. Asset identification

Asset identification is the first step in risk identification. Following the ISMS requirements, assets within the ISMS scope shall be identified prior to carrying out a risk assessment process [7]. There are two categories of assets as described in the ISO/IEC 27005; primary asset and supporting asset [9]. Primary assets are core business processes and their corresponding information whilst supporting assets are those required to be in place to support the activities of the primary assets. OCTAVE Allegro on the other hand has a different approach in asset identification. Its asset profiling is focused on information assets and their corresponding containers in which these assets lived [12]. The concepts used by the ISO/IEC 27005 and OCTAVE Allegro are similar i.e. information was identified as the key asset and other relevant assets were identified in relation to the information. For this work, both approaches were adopted and streamlined to assist in the asset identification.

TABLE I: TYPES OF ASSETS

Asset	Descriptions	Remarks
Information	Digital format/ printed on hardcopies i) Application data ii) System configuration files iii)System log files	Here, data is divided into three types to ensure consistent approach & understanding of the type of information that require protection. **Adoption & extension of:** a) Octave Allegro i) information asset ii) physical container b) ISO/IEC 27005 – i) primary asset: information ii) supporting asset: hardware
Data centre system	Applications and systems storing the 'Information' asset.	The system includes software and hardware. **Adoption & extension of:** a) Octave Allegro: i) technical container b) ISO/IEC 27005: i) supporting asset: software, hardware & network
Data centre infra	The physical location; data centre including general telecommunication equipment, utilities such as power, air –conditioning & humidity control.	**Adoption & extension of:** ISO/IEC 27005 i) supporting asset: site
People	The people involved with the information asset: Staff - internal Client & Contractor - external	**Adoption & extension of:** a) Octave Allegro – people container b) ISO/IEC 27005 – supporting asset: personnel

Taking a common and significant scope of ISMS implementation from Section III.A, an example of secure data centre is used to demonstrate the relationship concept derived for asset identification.

Table I listed the generic type of assets in a data centre, mapping them to how assets are being described in ISO/IEC 27005 and Octave Allegro.

At this stage, it is very important to fully understand and able to identify the assets involved and their corresponding types. Inaccurate asset identification with vague description of each asset type may lead to unnecessary efforts in the subsequent steps of the risk assessment. In Table 1, each of the asset type and its description is detailed and these descriptions are supported by the corresponding guidelines provided by ISO/IEC 27005 and Octave Allegro. The four types of assets above are proposed to be the set of assets for ISMS scope of a secure data center. The types of assets are explicitly set for the automation of the risk assessment exercise.

The relationship concept used for the asset identification phase above is designed to further eliminate complexity when it comes to threats and vulnerabilities identification. An experience risk analyst would be able to easily point out a potential repetition of risk exercises due to unstructured identification of assets. For the purpose of this paper, 'People' as an asset will not be included in rest of the discussion as it has a unique relationship which is addressed separately for the automation of the risk assessment. The relationship concepts are further discussed in the following section.

 ISBN: 978-1-61208-209-7

IV. ANALYSIS

In many ISMS implementations, the identification of assets was driven by organizational asset management process. This could pose as a challenge especially when the asset definitions and categorizations did not consider the information infrastructure which the organization had in place. This section discusses the analysis of the proposed relationships for the set of assets identified in Table I above. The discussion is limited to the scope of ISMS as discussed in Section III.A, i.e., secure data centre. The following relationships are demonstrated by ontology graphs which were generated using ontology editor, Protégé OWL.

A. *Relationship 1*

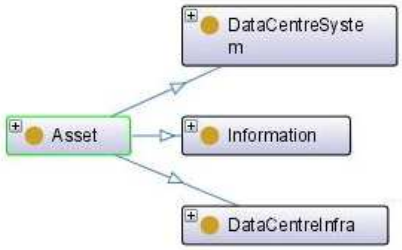

Figure 1. Assets within an ISMS scope

A secure data centre commonly housed key information asset. This asset is in digital format and requires corresponding hardware and software for it to be usable to an organization. These hardware and software components are defined as 'Data Centre System'.

The 'Data Centre System' requires a suitable environment for it to operate at its maximum capacity with minimal disruption. This environment is defined as 'Data Centre Infra'.

Thus the identified assets for ISMS scope of a secure data centre are Information, Data Centre System and Data Center Infra. Therefore, these three assets are subject to a risk assessment.

B. *Relationship 2*

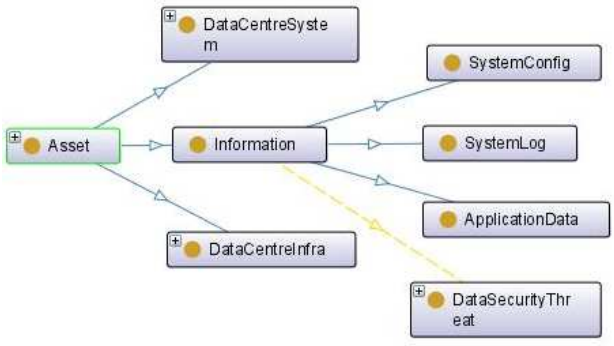

Figure 2. Information asset

The information asset of a secure data centre is further broken down into 'Application Data', 'System Configuration' and 'System Log'. These are important components of Information asset which are susceptible to threats related to information asset. The threats are defined as 'Data Security Threat'.

It is noted that up to this point, the relationships described are very common. It is however very significant to be discussed in this section as the rest of the relationships are based on these foundations.

C. *Relationship 3*

This relationship is for identifying threats for Data Centre System which is an asset of a secure data centre.

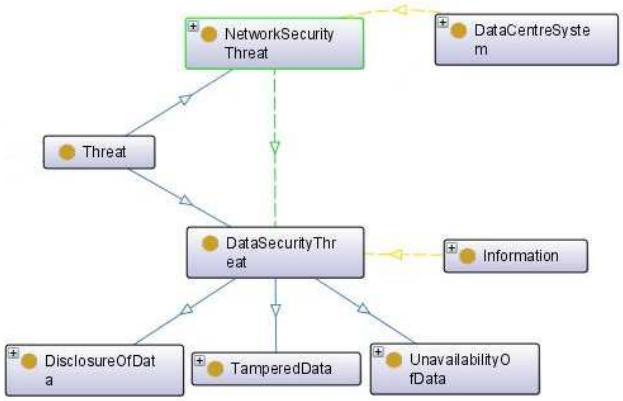

Figure 3. Threats

1) *Descriptions*

a) Two types of threats are shown in Figure 3; Network Security Threat and Data Security Threat

b) Data Security Threats are DisclosureOfData, TamperedData and UnavailabilityOfData

c) Network security threats are reconnaissance attacks, session attacks, unauthorized network access, DoS/DDoS (denial-of-service/ distributed denial-of-service) and malware attacks.

d) Network Security Threats are threats to Data Centre System.

e) Data Security Threats are threats to Information

f) Network Security Threats on Data Centre System resulted into Data Security Threats on Information

2) *Analysis*

a) "Network Security Threats" will eventually lead to threats on Information. This is justified due to the fact that Information resides in the Data Centre System and hence inherited the threats to the Data Centre System.

b) "Data Security Threats" are therefore inferred to be the results of "Network Security Threats".

 ISBN: 978-1-61208-209-7

c) This is an example of a relationship between data security threats and network security threats. Other relationships involving different types of threats might have the same results and will be used later in this study.

d) In a common risk assessment exercise, asset owners will need to be involved. Threat identification phase for an application owned by a business unit, may have the following scenario:

TABLE 2: THREAT IDENTIFICATION – A SCENARIO

Asset ID	**Asset Description**	**Asset Owner**	**Asset Type**
Asset 1	Business Application-System	Business Unit	Data centre system
Asset 2	Business Application-Application Data	Business Unit	Information
Asset 3	Business Application-System Log	Security Unit	Information

Guided by Relationship 1, Business Unit has identified both system (Asset 1) and data (Asset 2) as their assets. The latter could be unintentionally left out during an assessment as it could be assumed to be bundled in Asset 1 without specifying it explicitly and may result in an incomplete assessment. Next, with Relatioship 2, system log (Asset 3) has been identified by Security Unit which was not the main owner of the application.

Applying Relationship 3, unauthorized network access from a network security threat may be exploited by some vulnerabilities and could cause tampered data for Asset 2 and Asset 3. However, in a common risk assessment exercise, this threat may have only been identified for Asset 1 and the cascading impact on information asset residing in it might not be properly highlighted and analysed. Instead, a different set of assessment could have been carried out on information assets resulting in risk assessment results which were repetitive and lack of clarity.

e) Hence, Relationship 3 indicates that risk assessment could be conducted in a more structured manner whereby repetition of identifying threats for both Information and Data Centre System would be avoided.

V. CONCLUSION AND FUTURE WORK

Three relationship concepts have been discussed. These concepts were used to develop other relationships which have enabled the automation of risk assessment for an identified ISMS scope. An advisory system prototype was developed based on a risk assessment approach taken from the ISO/IEC 27005 to demonstrate the relationship concepts. Four types of assets were identified during the asset identification phase. However the threats identification phase had focused on two types of the assets namely Data Centre System and Information.

Future work will extend the relationships into selection of control measures to mitigate the identified risks.

VI. REFERENCES

[1] ISO/IEC, "ISO/IEC 27002 Code of practice for information security management," ISO/IEC, 2005.

[2] “The Top Cyber Security Risks”, (SANS Institute), [online] September 2009, http://www.sans.org/top-cyber-security-risks (Accessed: 29 March 2012).

[3] “Trial by fire”, (PWC), [online] 2009, http://www.pwc.com/giss2010 (Accessed: 25 April 2010).

[4] E. Humphreys, "Information security management standards: Compliance, governance and risk management," Information Security Technical Report, vol. 13, 2008, pp. 247-255.

[5] M. P. Kailay and P. Jarratt, "RAMeX: a prototype expert system for computer security risk analysis and management," Computers & Security, vol. 14, 1995, pp. 449-463.

[6] E. Humphreys, Implementing the ISO/IEC 27001 Information Security Management System Standard. Boston,London: ARTECH House, 2007, pp 21-25.

[7] ISO/IEC, "ISO/IEC 27001 Information Security Management Systems - Requirements," ISO/IEC, 2005.

[8] M. D. Aime, A. Atzeni, and P. C. Pomi, "AMBRA - Automated Model-Based Risk Analysis," in CCS: Conference on Computer and Communications Security (Proceedings of the 2007 ACM workshop on Quality of protection table of contents, SESSION: Risk analysis), Alexandria, Virginia, USA, 2007, pp. 43-48.

[9] ISO/IEC, "ISO/IEC 27005 Information security risk management," ISO/IEC, 2011.

[10] C. Jung, I. Han, and B. Suh, "Risk Analysis for Electronic Commerce Using Case-Based Reasoning," International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 8, 1999, pp. 61-73.

[11] G.-Y. Liao and C.-H. Song, "Design of a Computer-Aided System for Risk Assessment on Information Systems," in IEEE 37th Annual International Carnahan Conference on Security Technology, 2003, pp. 157-162.

[12] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007.

[13] H. Chivers, J. A. Clark, and P.-C. Cheng, "Risk profiles and distributed risk assessment," Computers & Security, vol. 28, 2009, pp. 521-535.

[14] “What is protégé?”, (protégé), [online] 2012, http://protege.stanford.edu (Accessed: 29 March 2012)

[15] “International Register of ISMS Certificates”, [online] 2012, http://iso27001certificates.com/ (Accessed: 29 March 2012)

 ISBN: 978-1-61208-209-7