Information Security Risk Management in Small-Scale Organisations: A Case Study of Secondary Schools Computerised Information Systems

[1] Moses Moyo
[1]School of Computing Science, UNISA
P. O. Box 392, Unisa 0003, Pretoria, South Africa
Email: mosesm50@gmail.com

[1]Hanifa.Abdullah
[1]School of Computing Science, UNISA
P. O. Box 392, Unisa 0003, Pretoria, South Africa
Email: abdulh@unisa.ac.za

[1]Rita C. Nienaber
[1]School of Computing Science, UNISA
P. O. Box 392, Unisa 0003, Pretoria, South Africa
ritanienaber101@gmail.com

Abstract—**The use of computerised information systems has become an integral part of South African secondary schools, bringing about a host of information security challenges that schools have to deal with in addition to their core business of teaching and learning. Schools handle large volumes of sensitive information pertaining to educators, learners, creditors and financial records, which they are obliged to secure. Unfortunately, school management and users are not aware of the risks to their information assets and the repercussions of a compromise thereof. Computerised information systems are susceptible to both internal and external threats but ease of access is likely to manifest in security breaches, thereby undermining information security. One way of enlightening schools about the risks to their computerised information systems is through a risk management programme. Schools may not have the full capacity to perform information security risk management exercises due to the unavailability of risk management experts and scarce financial resources. Therefore, the objective of this paper is to educate secondary schools' management and users on how to perform a risk management exercise for their computerised information systems in order to reduce or mitigate information security risks within their information systems and protect vital information assets. This study uses the Operationally Critical Threat, Asset, and Vulnerability Evaluation for small organisations (OCTAVE-Small) risk management methodology to address these information security risks in two selected secondary schools.**

Keywords: computerised information systems, risk, vulnerability, risk management, information security, threats, exposure, risk assessment, risk analysis.

I. INTRODUCTION

The proliferation of computerised information systems (CISs) in South African secondary schools has implications on information security in these organisations. There is no doubt that those secondary schools using CISs experience information security risk problems like any other small-scale organisation but may not be aware of such problems. Lack of proper risk management programmes may cause secondary schools to overlook essential information security requirements and this may lead them to use unsanctioned risk management strategies or even abandoning the programmes altogether. Risk management is a crucial component of information security practice because its outcome forms the basis upon which management makes decisions on what action to take on each identified risk [1]. Therefore, undermining information security risks has negative repercussions on abilities of schools to provide quality service. The continuing use of CIS in any organisation now depends on the quality of the information security risk management programme pursued by the organisation.

This paper proposes to conduct a risk management exercise in two South African secondary schools, in Vhembe District, Limpopo Province. The objective of this exercise is to educate school personnel with baseline computing skills who use CISs on how to manage information security risks and to secure their CISs. The study intends to utilise a qualitative case study in which the Operationally Critical, Asset, Threat and Vulnerability Evaluation for small organisations (OCTAVE-Small) risk management method will be used to assess risks in the selected schools' CISs. The study will customise the OCTAVE-Small processes to suit the CISs in secondary schools as well as the knowledge and skills of the users of these assets. Only CISs users from secondary schools with viable CISs will participate in this research study.

This paper is organised into eight sections. Section I provides an overview of information security risk management in secondary schools CIS. Section II, gives an insight into information security, highlights the security concerns in secondary schools information systems and suggests a solution to the inherent problems. Section III briefly discusses risk management, how to select a risk management method and types of risk management methods. Sections IV and V elucidate on the Operationally Critical, Asset, Threat and Vulnerability Evaluation (OCTAVE) risk management method and explore its potential use in secondary schools. Section VI examines the possible risk treatment approaches that schools could possibly apply, depending on the treatment strategies adopted. Benefits likely to be derived from this study are dealt with in Section VII. The paper's conclusion, Section VIII, reflects on the discussions made and highlights prospective steps for future research.

II. INFORMATION SECURITY

The importance of information security in secondary schools is increasing due to the greater usage of and reliance on computerised information systems. Information security is the protection of all elements that constitute an information system, namely hardware, software, information, people and processes [1],[1]. Information security is the practice of ensuring that information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so [3]. The major goal of information security in an organisation is to preserve the confidentiality, integrity and availability of information [1]. Confidentiality is the protection of information against theft and eavesdropping while integrity is the protection of information against unauthorised modification and masquerade [1]. Availability is the dependable access of authorised users to information, particularly in light of attacks such as denial of service against information systems [5]. Information security requires a range of skills and knowledge that are rarely found in small-scale organisations like secondary schools, an issue that this research attempts to address.

A. Source of security concerns in secondary schools' computerised information systems

Many secondary schools' CIS are supported by local area networks (LANs), which are normally connected to the Internet to provide access to the web. Personnel with baseline computing knowledge and skills administer these CISs. Administrative computers, holding vital and sensitive school information relating to educators, learners, creditors and financial records, are also part of these LANs. Educators and learners access these facilities, especially, when browsing the web and accessing e-learning material. The extent to which these information systems are secured is a matter of conjecture. There exists the need to encourage and educate information system users in secondary schools to regularly undertake risk management exercises, in order to reduce the exposure of critical information assets to risks from internal and external intruders.

B. Solution to the impending problem

Secondary schools need to put in place appropriate information security risk mechanisms to safeguard their CISs. The choice of information security mechanisms depends on the threats and exploitable vulnerabilities that exist in CISs [2]. This implies that secondary schools should conduct information security risk management exercises to assist the school management to explore various information security mechanisms that could be implemented in order to sustain these CISs. However, most secondary schools neither have expertise nor financial resources to perform risk management exercises. Therefore, there is a dire need for schools to be guided or assisted in performing risk management exercises, utilising the risk management methods that have the potential to educate users and management on how to manage risks in their CISs.

III. RISK MANAGEMENT

An information system asset is anything of value an organisation needs to utilise in order to accomplish its mission [6]. An asset can either be tangible or intangible [5]. Tangible assets include software, hardware and data while intangible assets include reputation, operations, trust and morale [5]. Information systems assets can be critical or non-critical depending on the importance of the operations each asset is supporting [7], and these vary from organisation to organisation [5]. Information systems assets can be at risk, compromising information integrity, confidentiality and availability. A risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset [6]. In this regard, a risk is the potential for an unwanted event to occur and is a function of the likelihood of that unwanted event occurring and its consequences [8]. A risk arises from three conditions called risk factors (contextual problems), namely the existence of a threat (hazard), exposure of an asset to that threat and the vulnerability of the asset [9]. A threat is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm information, operations, the environment, and/or property [1],[10]. The existence of a threat implies that there exists the capability and intention of an adversary to undertake actions that could be detrimental to an organisation's interests [1]. An information security exposure may be a system configuration issue, mistake in software or a problem according to some reasonable security policy that allows access to information or capabilities that can be used by an attacker as a stepping stone into the system or network [11]. Vulnerability is a combination of the attractiveness of a facility as a target and the level of deterrence and (or) protection provided by the existing countermeasures [12]. Therefore, vulnerability is the degree to which the exposed elements of an information system will suffer a loss from the impact of a threat. All assets are exposed to some degree of risks which the owners of assets may be unaware of. Therefore, by participating in risk management exercises, CISs users in secondary schools will be aware of information assets that are at risk and the type of threats as well as vulnerabilities that lead to risk situations.

Risk management is a basic management activity that helps an organisation to meet its objectives through the allocation of resources to undertake planning, make decisions, and carry out productive activities [13]. Risk management differs from other management activities because it deals with uncertainties that an organisation faces. The uncertainties include the occurrence of harmful events and the value to the organisation of consequences of such events [13]. Secondary schools are encouraged to carefully manage uncertainties using sanctioned risk management methods that are within their means.

The two major activities of risk management are risk assessment and analysis [7],[1]. Risk assessment is the process of identifying, characterising, and understanding risk; that is, studying, analysing, and describing the set of outcomes and likelihoods for a given endeavor [10],[14]. Risk analysis involves further identification of security risks, determining their magnitude and identifying the corresponding areas that

need safeguards [6]. For secondary schools to partake in risk management there is a need for the management and users to have basic knowledge and skills on these risk management facets.

A. Choice of risk management process

The choice of a risk management method depends on the understanding and appropriate application of that method in a given organisational context. This area is difficult particularly to resource and expertise-constrained small-scale organisations [1]. This situation is even worse in secondary schools where personnel with baseline computing skills are only concerned with the use of CISs regardless of the perennial security risks associated with these information systems assets. In light of this, secondary schools need assistance from within or outside the organisation to initiate and guide them in performing risk management for their CIS.

B. Types of risk management methods

Risk management methods can be quantitative or qualitative, depending on the risk assessment and analysis applied [16]. Quantitative information security risk management methods draw upon methodologies used by financial institutions and insurance companies [1],[17]. Popular examples of quantitative risk assessment and analysis methods include the Annualised Loss Expectancy (ALE) and the Livermore Risk Analysis Methodology (LRAM) [1],[1],[10]. These methods use numerical results that express the probability of each risk factor and its effects on the objectives of the organisation [16]. Quantitative methods are suitable for large information systems infrastructure supported by strong human and financial resources [18]. Organisations that use quantitative methods capitalise on these methods objectivity because they depend on mathematical formulae that can easily be verified [1]. Quantitative methods rely on estimations of the probability of damages or loss of information systems assets [1],[19]. This makes them problematic to use in small-scale organisations such as secondary schools where there is no risk management expertise to perform such complex estimations. Rot [20] argues that a risk management exercise conducted using quantitative method is generally more expensive and demands greater experience and more advanced tools than those conducted using qualitative methods. Due to these constraints, small organisations, like secondary schools lack the capacity to use quantitative risk management methods. Hence, qualitative methods become an alternative.

Qualitative risk management involves the assessment of the effects of the identified risk factors and the creation of priorities that can be used to decide on how to solve the potential risk factors, depending on the impact they could have on the information systems assets [16]. Most qualitative methods can be modified for easy use with any expertise available in an organisation [18]. Their simplicity arises from the fact that they express risks in terms of descriptive variables or adjectives instead of precise monetary terms, therefore, requiring less time, finance and effort to implement [1]. This makes them simple because they utilise the 'jargon' which non-technical people are familiar with. Furthermore, qualitative methods are based on judgment, intuition and experience of the individual(s) who conducts the risk management exercise [17]. This makes qualitative risk management methods a better choice for use in secondary schools where there are no risk management personnel.

A number of identified qualitative risk assessment and analysis techniques also pose serious problems in secondary schools due to some complexities. For example, the Hazard And Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) or Failure Mode and Effects Criticality Analysis (FMECA) and the Central Computer and Telecommunications Agency, CCTA-Risk Analysis and Management Method (CRAMM) require a highly trained technical team to perform risk assessment and analysis, are labour intensive or require strong financial bases [20]. This makes the use of these methods unsuitable for schools due to lack of these resources. However, not all qualitative risk assessment and analysis techniques require highly technical people or strong financial support. For example, the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) technique provides an easy, cheap and viable means of achieving the same objectives that any of the other methods is capable of [21],[22].

Among the commonly cited examples of qualitative risk management methods is the OCTAVE, which has been found to be the most appropriate for use in organisations where there are no experts in information risk management [23]],[18].

Some risk management techniques are either too difficult to understand or use by small-scale organisations, with the result that these organisations may succumb to unsanctioned methods or avoid carrying out risk management exercises completely [23],[1]. To encourage secondary schools to perform risk management, a simple and participatory risk management method in the qualitative category, OCTAVE-Small, is recommended.

IV. OVERVIEW OF OCTAVE-SMALL

Secondary schools require risk management methods that enable management and users to be acquainted with their CISs security issues so that they can improve their security posture without reliance on outside experts. The OCTAVE method seems to be the most appropriate choice for this purpose. The OCTAVE risk management method is a process-driven methodology that identifies, prioritises and manages information security risks within an organisation's information system [22],[18]. This method is designed to provide complete information for information security risk management [21]. OCTAVE is self-directed because it encourages people from within the same organisation to collaboratively assume the responsibility of setting the organisation's security strategy [18], an outcome this study seeks to achieve.

Variations of the OCTAVE method offer an organisation a choice of the risk management techniques suitable to the organisation depending on the size and layering of its information systems [18]. Secondary schools typically have a flat-layered hierarchical structure, therefore, their information systems can be assessed and analysed using OCTAVE for

Small organisations (OCTAVE–Small) method. Alberts and Dorofee [21] and Sosonkin [24] argue that by implementing the OCTAVE-Small risk management process, an organisation tends to benefit on: a catalogue of practices - a collection of good strategic and operational security practices; a threat profile - the range of threats that an organisation needs to consider; and a catalogue of vulnerabilities - a collection of vulnerabilities based on platform and application. These catalogues can act as references for secondary schools that decide to embark on a risk management exercise using personnel with baseline computing skills.

This study capitalises on the flexibility of the OCTAVE-Small depicted by Figure 1 which has been customised to secondary schools' unique risk environments, security and resiliency objectives and the skill level available. Customisation of the conventional OCTAVE-Small will involve trimming the activities that require extensive paper work like the threat-profile trees in Process 2. These will have to be replaced by simplified observation and inspection checklists based on users' daily experiences and level of understanding. Activities will be rearranged so that there is no repetition of similar activities in different processes. Critical information systems assets will be determined in Process 1 instead of Process 2. It is better that while the team is identifying and locating assets, the team immediately selects the critical assets. This is intended to make the risk management exercise user friendly and interesting to the school personnel and at the same time answering the following five basic information security risk questions.

- What information CISs assets in secondary schools require protection?
- What threats or vulnerabilities should the schools' CIS assets be protected against?
- What is the level of information security breaches in these CIS assets?
- What level of protection is needed to mitigate risks?
- What is the impact on a CIS if the existing protection fails?

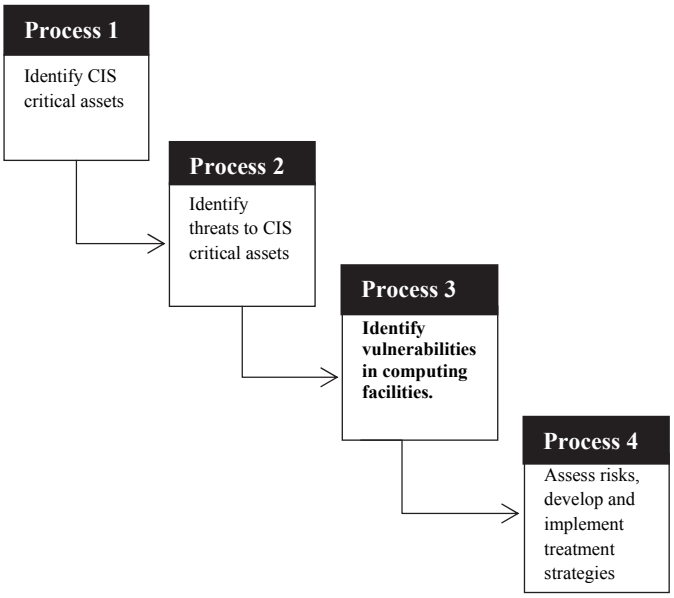

Figure 1: OCTAVE-Small risk management process

V. IMPLEMENTING OCTAVE-SMALL METHOD IN SECONDARY SCHOOLS

When using the OCTAVE-Small, a collaborative team has the responsibility of conducting risk management exercise in selected schools. Each collaborative team comprises of three to five key users of the CISs selected from each school by the school management in consultation with CISs users. Such team members are expected to have a deep understanding of the operations of their schools. After obtaining approval from each School Management Team (SMT) the collaborative team will start the implementation of the risk management exercise. The team leader leads the team, while another member documents all daily transactions for each process undertaken. The collaborative team will carry out the activities as described under each process in Figure 1. Data will be collected using observation and inspection checklists, interview schedules, customised OCTAVE-Small worksheets and some supplementary worksheets designed for this purpose. Data will be qualitatively processed, presented and interpreted.

A. Process 1: Identifying critical CIS assets and their protection requiremnts.

A collaborative team will comprise mainly of the regular users of the CISs in schools lead by the researcher. The users of the CISs in the collaborative team know where different information assets are located and will provide all the required information about the information assets at their schools. Each team will then examine the security status of each identified critical asset taking into account the immediate environment of that asset. School information security policy and other related policies will be studied if they are availed. During this process the team leader will assist the other members on how to collect the necessary data and record this data on the worksheets. The team will then construct a list of critical

assets for the schools' CISs. By participating in this process, users of CISs will be provided with an opportunity to learn to identify critical assets based on given information about a group of information systems assets.

B. *Process 2: Identifying threats to critcal CIS assets*

The main activity in this process is the checking of existing protection mechanisms that are in place for each identified critical CISs asset. The team further examines who accesses the asset, how it is accessed, when is it accessed, why is it accessed in that way, what security breaches are likely to take place and their effect on the confidentiality, integrity and availability of the information stored in that asset. The team leader will also observe how the systems are being used and then interview system users. Users of the CISs should be able to identify threats to critical assets they are using.

C. *Process 3: Identifying vulnerabilities in computing facilities.*

The team will physically inspect all computing facilities concentrating on hardware, systems software and specialised application software configurations. Malware and simple vulnerability scans will be performed on selected workstations and the network. All identified vulnerabilities in the computing facilities will be documented. Visible threats to the assets will also be documented. The team will also examine the databases, and network infrastructure in the schools. The team leader will educate the other team members on the implications of the shortfalls identified. After completing this activity, users of CISs should be able to identify and describe vulnerabilities in their CISs assets.

D. *Process 4: Assessing risks, developing and implementing treatment strategies.*

The team will assess risks using the information gathered in the first three processes. A qualitative risk metric (Table 1) [2] will be used to guide the team in this process. Risks or threat sources are identified, analysed and their impact on concerned information systems evaluated too. The matrix uses qualitative descriptive terms, high, medium and low as determined by the collaborative team. The risks are categorised according to their impact on the operations of the schools. The team then recommends on what treatment should be adopted. Based on these findings, the team will develop a protection strategy based on the identified risks that each school could implement. Upon completing this process, each participating user is expected to perform simple risk analysis and come up with a protection strategy for an affected asset.

TABLE I. QUALITATIVE RISK ANALYSIS MATRIX

	LIKELIHOOD		
CONSEQUENCES	**Low**	**Medium**	**High**
High	M	H	H
Medium	L	M	H
Low	L	L	M

Key: H: high risk
M: medium risk
L: low risk

VI. RISK TREATMENT

Risk treatment is a process that consists of selecting and applying the most appropriate risk security measures or controls in order to modify the risk, with the aim of avoiding the damages intrinsic to the risk factor or of making use of the advantages it could provide to the organisation [24],[14]. This study aims to equip all users who participate in the study with basic knowledge and skills in risk treatment. Four prominent risk treatment strategies that are commonly used, are risk avoidance, acceptance, transference and treatment [7],[1]. Before the school management decides on which risk treatment to adopt, the users and management must be educated on the implication of the option and the likely consequences. Central to all risk treatment methods will be the role played by the users of CISs to information security risks. Based on the outcome of the risk assessment process, the risks arising from the users' contributions will be highlighted and ways of reducing such risks explored.

VII. BENEFITS DERIVED

Security training and awareness among users of CISs is an essential component of information security risk management for an organisation [21]. This study will provide participants with an opportunity to develop an appreciation of information security in general and how to manage risks associated with their CIS in particular. It will also develop and foster a sense of responsibility and accountability in those users who previously were deliberately involved in activities that led to security breaches to their schools' CISs. Schools will have s to rely on some individuals to improve their CIS security posture. Management will utilise these users to make meaningful decisions on CIS risks related issues.

VIII. CONCLUSION AND FUTURE RESEARCH

Curtailing information security risks in secondary schools should be treated seriously as computerisation in schools escalates. These information systems may become the source of future insecurities or platforms from which security threats emanate. Secondary schools that use CISs should remain as secure as possible to safeguard their operations.

This paper discussed the prospects of conducting a risk management exercise in secondary schools that use CISs. The research will be carried out in Vhembe District, Limpopo Province. The purpose of the research is to educate users and school management on the best practice of information security for their CIS. The research utilises a customised OCTAVE-Small risk management process which users with baseline information technology skills and knowledge are likely to appreciate. CISs users who will participate in this study are expected to receive basic information security and awareness training so that they able to perform basic information security risk management in their respective schools. The final results of this research project/study will be reported on in subsequent publications. This study will serve as a basis for future research in the use of information systems in small-scale organisations looking at other important aspects.

REFERENCES

[1] B. Karabacaka, and I. Sogukpinar, "ISRAM: information security risk analysis method". Computers and Security Volume 2003 24, pp. 147 - 159.

[2] J. Beachboard, A. Cole, M. Mellor, S. Hernandez and K. Aytes, "Improving information security risk analysis practices for small and medium sized enterprises. A research Agenda." 2008. Issues in Information Sciences and Technology Volume 5, 73 - 85.

[3] S. Elky, "An Introduction to Information System Risk Management." May 31, 2006 SANS Institute InfoSec Reading Room SANS Institute 2007. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204. (Accessed on 29 June 2011).

[4] M. J. S. Kite, "Information Security Policy" 2009. Retrieved from http://www.abdn.ac.uk/hr/uploads/files/information-security-policy.pdf (Accessed on 23 June 2012)

[5] M. Theoharidou, S. Kokolakis, M. Karyda and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799". Computers and Security Volume 24, Issue 6, pp 472-484, 2005,

[6] M. T. Chen, "Information Security and Risk Management." Encyclopaedia of Multimedia Technology and Networking, 2nd ed., M. Pagani (ed.), Idea Group Publishing, 2009. Retrieved from http://lyle.smu.edu/~tchen/papers/info-sec-risks.pdf. (Accessed 15 March 2012).

[7] Z. Ciechanowicz, "Risk analysis: requirements, conflicts and problems" Cornpurer.\ and Srcuriq, Vol. 16. No. 3, pp. 223-232, 1997. Elsevier Science Ltd. Retrieved, 1997. from ftp://163.25.117.117/gyliao/TODylan/Risk%20analysis-%20requirements_conflicts%20and%20problems.pdf (Accessed on 23 January 2013)

[8] L. Dorian "Risk Management: Understanding Industry Insights", 2012 Retrieved from http://www.ica.bc.ca/ii/ii.php?catid=17. (Accessed on 25 February 2012)

[9] T. Siu "Information Scecurity Risk management", 2007. Retrieved From http://wiki.edu/information_security_risk_kanagement:Overarching_themes. Accessed on 31 March 2011

[10] G. Pare, C. Sicotte, M. Jaana and M.S.D. Girouard, "Prioritizing Clinical Information System Project Risk Factors" A Delphi Study proceedings of the 41st Hawaii International Conference on System Sciences, 2008

[11] R.K. Rainer, C.A. Snyder and H. H. Carr, H. HRisk analysis for information technology. Journal of Management Information Systems. Volume 8 Numeber 1., 129 – 147, 1991.

[12] A. Tiwari, "Information Security Risk Management: An Overview Risk Management: An Essential Guide to Protecting Critical Assets" 2010. Retrieved from http://www.suite101.com/profile.cfm (Accessed on 23 September 2012).

[13] N.A. Renfroe and J.L. Smith, "Threat/Vulnerability Assessments and Risk Analysis." Applied Research Associates, Inc, 2010. Retrieved from http://www.wbdg.org/resources/riskanalysis.php#top (Accessed on 25 January 2013)

[14] J. Shortreed, J. Hicks and L. Craig "Basic Frameworks for Risk Management", Final Report March 28, 2003 Prepared for The Ontario Ministry of the Environment, 2003. Retrieved from http://www.irrneram.ca/pdf_files/basicFrameworkMar2003.pdf. (Accessed on 26 May 2012)

[15] K. J. Soo Hoo, "How much security is enough? A risk-Management approach to computer security" - A working paper. Consortium for research on Information security and Policy. 2000. Retrieved from http://wwww.cisac.stanford.edu/publications/how_much_is_enough__a_risk_management_approach_to_computer_ security.pdf. (Accessed on 14 February 2011).

[16] V. Mazareanu, "Risk Management and Analysis: Risk Assessment Qualitative and Quantitative" 2007. Retrieved from http://papers.ssrn.com/sol13/papers.cfm?abstractid=1549186. (Accessed on 2 September 2011)

[17] C.C. Lo, and W.J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls". Expert Systems with Applications 39 247–257, 2012

[18] P. Panda, "The OCTAVE approach to information security risk assessment. Journal of Past Issues Vol 4, pp. 20 - 25 , 2009. Retrieved from http://www.isaca.org.Journal/past-issues/2009/volume4/documents/jpdf09-OCTAVE.pdf (Accessed on 2 May 2013)

[19] T. Ding, "Quantitative Risk Analysis Step-by-step. GSEC Practical Version", 2002.. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849. (Accessed on 12 April 2011).

[20] A. Rot, "IT Risk Assessment: Quantitative and Qualitative Approach". World Congress on Engineering and Computer Science WCECS pp. 22-24. San Francisco: SANS, 2008.

[21] C. Alberts and A. Dorofee, "Managing information security risks: The OCTAVE SM approach". Boston: Addison-Wesley Anderson, 2002.

[22] C. Alberts and A. Dorofee, "Using Vulnerability Assessment Tools to Develop an OCTAVE Risk Profile". SAN InforSecurity 2004. Retrieved from http://www.fish.com/satan/admin-guide-to-cracking.html. (Accessed on 25 February 2011)

[23] C. Alberts and A. Dorofee, "An introduction to OCTAVE SM Method" 2001. Retrieved from http://www.cert.org/octave/methodintro.htm/#intro. (Accessed on 25 February 2011)

[24] M. Sosonkin, "OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation", CS996: Information Security Management Polytechnic University, 2005. Retrieved from http://isis.poly.edu/courses/cs996-management-s2005/Lectures/octave.pdf (Accessed on 25 September 2012).

[25] J. Shortreed, "ISO 31000 – Risk Management Standards", 2008. Retrieved from http://www.irr-neram.ca/pdf_files/ISO%2031000.pdf (Accessed on 27 May 2012