CONTROL PRIORITIZATION MODEL FOR IMPROVING INFORMATION SECURITY RISK ASSESSMENT

NADHER MOHAMMED AL-SAFWANI

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2014

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Penilaianaset tertentu untuk penilaian risiko keselamatan maklumat perlu mengambil kira kewujudan sumber yang mencukupi dan pulangan ke atas pelaburan (ROI). Walaupun rangka kerja penilaian risiko yang baik diperlukan, kebanyakan rangka kerja yang sedia ada tidak mempunyai garis panduan terperinci dan kebanyakannya bergantung kepada kaedah kualitatif. Oleh itu, ia memerlukan tambahan masa dan kos untuk menguji semua kawalan keselamatan maklumat. Kebersandaran kepada input dan maklum balas manusia akan meningkatkan penentuan subjektif dalam organisasi. Matlamat utama tesis ini adalah untuk mereka bentuk model Keutamaan Kawalan Keselamatan Maklumat (ISCP) yang efektif bagi memperbaiki proses penilaian risiko. Kajian kes berdasarkan ujian penembusan dan penilaian kerentanan telah dilaksanakan untuk mengumpul data. Kemudian, Teknik untuk Susunan Prestasi dengan Keserupaan kepada Penyelesaian Ideal (TOPSIS) telah digunakan untuk menentukan keutamaan data. Gabungan analisis kepekaan dan temuduga pakar telah digunakan untuk menguji dan mengesahkan model ini. Seterusnya, prestasi model tersebut telah dinilai oleh pakar keselamatan. Hasil penyelidikan ini menunjukkan model ISCP telah meningkatkan kualiti penilaian kawalan keselamatan maklumat dalam organisasi. Model ini memainkan peranan penting untuk menentukan keutamaan kawalan keselamatan teknikal yang kritikal semasa proses penilaian risiko. Tambahan pula, output model ini menyokong perlaburan keselamatan dengan mengenal pasti kawalan yang sesuai untuk mengurangkan risiko ke tahap yang boleh diterima dalam organisasi. Sumbangan utama kajian ini adalah pembangunan satu model yang mengurangkan ketidak-tentuan, kos dan masa penilaian kawalan keselamatan maklumat. Panduan yang praktikal dan jelas akan membantu organisasi untuk menentukan keutamaan kawalan penting dengan lebih cekap dan dipercayai. Semua sumbangan ini akan meminimakan pembaziran sumber dan memaksimakan keselamatan organisasi.

Kata kunci: Penilaian risiko keselamatan maklumat, pengurusan risiko, proses penilaian, keutamaan kawalan keselamatan.

Abstract

Evaluating particular assets for information security risk assessment should take into consideration the availability of adequate resources and return on investments (ROI). Despite the need for a good risk assessment framework, many of the existing frameworks lack of granularity guidelines and mostly depend on qualitative methods. Hence, they require additional time and cost to test all the information security controls. Further, the reliance on human inputs and feedback will increase subjective judgment in organizations. The main goal of this research is to design an efficient Information Security Control Prioritization (ISCP) model in improving the risk assessment process. Case studies based on penetration tests and vulnerability assessments were performed to gather data. Then, Technique for Order Performance by Similarity to Ideal Solution (TOPSIS) was used to prioritize them. A combination of sensitivity analysis and expert interviews were used to test and validate the model. Subsequently, the performance of the model was evaluated by the risk assessment experts. The results demonstrate that ISCP model improved the quality of information security control assessment in the organization. The model plays a significant role in prioritizing the critical security technical controls during the risk assessment process. Furthermore, the model's output supports ROI by identifying the appropriate controls to mitigate risks to an acceptable level in the organizations. The major contribution of this research is the development of a model which minimizes the uncertainty, cost and time of the information security control assessment. Thus, the clear practical guidelines will help organizations to prioritize important controls reliably and more efficiently. All these contributions will minimize resource utilization and maximize the organization's information security.

Keywords: Information security risk assessment, risk management, assessment process, security control prioritization.

Declaration Associated with This Thesis

Some of the works presented in this thesis have been published or submitted as listed below.

[1] **Nadher Al-Safwani,** Suhaidi Hassan and Norliza Katuk, On Multi Attribute Decision Making Methods: Prioritizing Information Security Controls, Journal of Applied Sciences, Vol. 14(16), pp. 1865-1870 (2014), ISSN: 1812-5654. [Citation indexed by ISI web of knowledge and SCOPUS]

[2] **Nadher Al-Safwani,** Suhaidi Hassan and Norliza Katuk, A Multiple Attribute Decision Making for Improving Information Security Control Assessment. International Journal of Computer Applications, Vol. 89(3), pp. 19-24 (2014).

[3] **Nadher Al-Safwani,** Suhaidi Hassan and Norliza Katuk, ISCP: In-Depth Model for Selecting Critical Security Controls. American Journal of Engineering and Applied Sciences, Under review.

Acknowledgements

In the name of ALLAH, Most Gracious, Most Merciful:

"*Work; so Allah will see your work and (so will) His Messenger and the believers*;"

(The Holy Quran - AtTawbah 9:105)

Although PhD work is a lonely journey of individual endeavour, this study would not have come to fruition without the support of many people, to whom I am sincerely indebted. My deepest gratitude is to my supervisors, Professor Dr Suhaidi Hassan and Dr Norliza Katuk, for their continuous guidance, fruitful feedback, moral support, and sharing of all their research experiences throughout these challenging years. They have willingly provided not only advice and constructive comment but also optimism and encouragement during difficult times. Their detailed and constructive comments have helped me to better shape my research ideas.

My gratitude also goes to all my colleagues throughout the PhD including during the monthly research camps; among them are Dr Ahmad Suki, Dr Adib Habbal, Dr Yaser Miaji, Dr Mohd. Hasbullah, and many others, specifically for the discussions and sometimes the heated arguments on better ways to perform research. They not only contributed constructive ideas on my research work, but also read my thesis.

Good friends are a true blessing. I am fortunate enough to have a circle of friends who provided the much needed respite while I pursued this lofty goal. I would like to thank Anis, Abdullah, Sazly, Fazil, Nouman, Abdul Alem, Yousef and Mohammed Gamal for being such a close part of our lives. Also, I would like to thank Belal who touched my life over the last few years and helped me directly and indirectly with his outstanding advice on personal development.

Completing a PhD is a gruelling proposition and impossible but for the support and

encouragement of family. I would like to offer my heartfelt thanks to my father Mr Mohammed Al-Safwani, my mother Mrs Fawzia Osman, and to my sisters and brothers.

And finally, but most importantly, I would like to thank my wife Dhekra. She supported me at times when I could not keep myself going and tolerated me when I spent many hours a days engrossed in my research, while abdicating my responsibilities as a husband. The thought of seeing the pride on her face as I receive my degree kept me going. Thank you for always being there for me, for your unrequited support and for being an inexhaustible source of happiness and affection.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

AHP	Analytic Hierarchy Process
CAPEX	Capital Expenditure
COBIT	Control Objectives for IT and Available Technology
DRM	Design Research Methodology
DS-I	Descriptive Study-I
DS-II	Descriptive Study-II
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability
EBIOS	Expression of Needs and Identification of Security Objectives
GAIA	Geometrical Analysis for Interactive Assistance
HAW	Hierarchical Adaptive Weighting
IRAM	Information Risk Analysis Methodology
ISCP	Information Security Control Prioritization
ISRA	Information Security Risk Assessment
ISRM	Information Security Risk Management
ISMS	Information Security Management System
ISO	International Organization of Standards
MADM	Multi Attribute Decision Making
MEW	Multiplicative Exponential Weighting
NIST	National Institute of Standard and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OPEX	Operational Expenditure
PS	Perspective Study
PROMETHEE	Preference Ranking Organization Method for Enrichment Evaluations
RC	Research Clarification
ROSI	Return on Security Investment
SRM	Security Risk Management
SDLC	System Development Life Cycle
SAW	Simple Adaptive Weighting
TOPSIS	Technique for Order Performance by Similarity to Ideal Solution

CHAPTER ONE
INTRODUCTION

The main aim of an information system for businesses is to enhance their operation and to facilitate decision making. This electronic dependency has improved business operations and opportunities [13, 14]. Information Security Risk Management (ISRM) is playing a critical role not only in exploring and assessing information security risks to business operations, but also in determining the appropriate controls. This research presents an Information Security Control Prioritization (ISCP) model which improves the control assessment process in ISRM. This chapter is an overall introduction to the thesis, initially outlining the Information Security Risk Assessment (ISRA) framework and its steps. It then establishes the strategy, direction, motivation, importance and contributions of the research. Section 1.1 gives a brief background of the research focus and general goal. The research motivation is described in Section 1.2, followed by discussion of the research problem, research questions and research objectives in Sections 1.3, 1.4, 1.5 respectively. The scope and flow of the research are described in Sections 1.6 and 1.7 respectively. The last two Sections discuss the research contributions and organization of the thesis.

1.1 Information Security Risk Assessment Frameworks

The Internet has become the main resource for information searching around the globe; however, it presents many challenges and raises many issues to organizations in managing their assets. Organizations depend on information that is accessed over the networks and is stored in digital formats, making it their most valuable asset [2, 15]. Hence, security and protection of information assets are becoming of utmost importance for organizations and businesses. Lack of security opens organizational assets, particularly sensitive information and critical systems, to a variety of risks such as loss,

The contents of the thesis is for internal user only

REFERENCES

[1] F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating security controls based on key performance indicators and stakeholder mission," in *4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*. Oak Ridge, Tennessee: ACM, May 2008, pp. 1–11.

[2] E. Wheeler, *Building an Information Security Risk Management Program from the Ground Up*, E. Wheeler, Ed. Waltham, 2011.

[3] W. H. Baker and L. Wallace, "Investigating quality in information security management," *IEEE Security & Privacy*, vol. 5, pp. 36–44, 2007.

[4] T. R. Peltier, *Information Security Risk Analysis, Third Edition*, Auerbach, Ed. Northwest,USA: Auerbach Publications, 2010.

[5] R. Ross, A. Johnson, S. Katzke, P. Toth, G. Stoneburner, and G. Rogers, *Guide for Applying the Risk Management Framework to Federal Information Systems*, U.S. Department of Commerce Std., 2010.

[6] A. Singh, "Improving information security risk management," PhD, Minnesota University, Saint Paul, Minnesota, December 2009.

[7] WASC, "Wasc threat classification," Web Application Security Consortium, Tech. Rep., 2010.

[8] J. Meier, A. Mackman, and B. Wastell, *Threat Modeling Web Applications*, Microsoft Patterns & Practices Library, May 2005, mSDN. [Online]. Available: http://msdn.microsoft.com/en-us/library/aa302419.aspx#c03618429_011

[9] ISO/IEC, *ISO 27005 Information Technology Security Techniques Information Security Risk Management*, BSI Information Security 27 005, Rev. 1, 2008.

[10] G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*, NIST Std., 2002.

[11] ISO/IEC, *Risk Management: Risk Assessment Techniques*, IEC/FDIS 31010 Std. 31 010, 2009.

[12] M. Walker, "Ec-council training ceh v7," http://www.eccouncil.org/Training, June 2012.

[13] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies: A contextual perspective," *Computers & Security*, vol. 24, no. 3, pp. 246 – 260, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404804002378

[14] R. L. Winkler, "Uncertainty in probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 54, pp. 127 – 132, 1996, <ce:title>Treatment of Aleatory and Epistemic Uncertainty</ce:title>. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832096000701

[15] S. P. Bennett and M. P. Kailay, "An application of qualitativerisk analysis to computer security for the commercial sector," in *Computer Security Applications Conference, Eighth Annual*. San Antonio, Texas: IEEE, 1992, pp. 64–73.

[16] M. Wright, "Third generation risk management practices," *Computer Fraud & Security*, vol. 2, pp. 9–12, 1999.

[17] T. R. Peltier, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, A. Pub, Ed. New York,USA: Auerbach Pub, 2002.

[18] S. N. Foley, "Security risk management using internal controls," in *workshop on Information security governance*. Chicago, Illinois, USA: ACM, November 2009, pp. 59–63.

[19] F. Farahmand, W. J. Malik, S. B. Navathe, and P. H. E. and, "Security tailored to the needs of business," in *The Proceeding of the ACM CCS Workshop on Business Driven Security Engineering*. Fairfax, VA: ACM CCS Workshop, 2003.

[20] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002. [Online]. Available: http://doi.acm.org/10.1145/581271.581274

[21] N. Honghui and S. Yanling, "Research on risk assessment model of information security based on particle swarm algorithm rbf neural network," in *Circuits,Communications and System (PACCS), 2010 Second Pacific-Asia Conference on*, vol. 1, aug. 2010, pp. 479 –482.

[22] NIST, *Minimum Security Requirements for Federal Information and Information Systems*, U.S. DEPARTMENT OF COMMERCE Std., 2009.

[23] L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Commun. ACM*, vol. 49, no. 1, pp. 121–125, Jan. 2006. [Online]. Available: http://doi.acm.org/10.1145/1107458.1107465

[24] A. Singh and D. Lilja, "Improving risk assessment methodology:a statistical design of experiments approach," in *4th International Conference Security of Information and Networks (SIN 2011)*. Sydney, Australia: ACM, October 2009, pp. 21–29.

[25] E. Papadaki, D. Polemi, and D. K. Damilos, "A holistic, collaborative, knowledge-sharing approach for information security risk management," in *Proceedings of the 2008 The Third International Conference on Internet Monitoring and Protection*, ser. ICIMP '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 125–130. [Online]. Available: http://dx.doi.org/10.1109/ICIMP.2008.19

[26] J. Breier and L. Hudec, "Risk analysis supported by information security metrics," in *12th International Conference on Computer Systems and Technologies*. Vienna, Austria: ACM, 2011, pp. 393–398.

[27] S. Lauesen and H. Younessi, "Six styles for usability requirements," in *Proceedings of the Fourth International Workshop on Requirements Engineering: Foundation for Software Quality: REFSQ'98*. Pisa, Italy: Presses Universitaires de Namur, 1998, pp. 155–166.

[28] K. Papadaki and N. Polemi, "Towards a systematic approach for improving information security risk management methods," in *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium*. Athens, Greece: IEEE, 2007, pp. 1–4.

[29] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, jan. 2009, pp. 1 –10.

[30] J. Mounzer, T. Alpcan, and N. Bambos, "A quantitative model for security risk management in information technology intensive organizations," Standford University, Stanford, California, Tech. Rep., 2007.

[31] I. G. Institute, *COBIT4.1*, ISACA, Ed. Rolling Meadows,USA: IT Governance Institute (ISACA), 2007.

[32] A. D. Veiga and J. H. P. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/10580530701586136

[33] SANS, "Twenty critical security controls for effective cyber defense: Consensus audit guidelines," SANS, Tech. Rep., 2011.

[34] R. M. Schneider, "A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques," in *2010 Information Security Curriculum Development Conference*, ser. InfoSecCD '10. New York, NY, USA: ACM, 2010, pp. 107–116. [Online]. Available: http://doi.acm.org/10.1145/1940941.1940966

[35] W. Dariusz, "Information security risk assessment model for risk management," in *Trust and Privacy in Digital Business*, ser. Lecture Notes in Computer Science, S. Fischer-HAbner, S. Furnell, and C. Lambrinoudakis, Eds. Springer Berlin / Heidelberg, 2006, vol. 4083, pp. 21–30. [Online]. Available: http://dx.doi.org/10.1007/11824633_3

[36] *A Reuse-Based Approach to Determining Security Requirements*. Citeseer, 2003.

[37] G. Locke, *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Std., Rev. NIST 800-53, 2009.

[38] Y. Beres, A. Baldwin, and S. Shiu, "Model-based assurance of security controls," in *2007 ACM workshop on Quality of protection*. Alexandria, Virginia, USA: ACM, 2007.

[39] C. Andersen, "Successful security control selection using nist sp 800-53," *ISSA Journal*, vol. 1, pp. 12–17, 2009.

[40] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "Assessing damages of information security incidents and selecting control measures, a case study approach," in *Fourth Workshop on the Economics of Information Security,WEIS05*. Kennedy School of Government, Harvard University: Citeseer, 2005.

[41] K. Stolen, F. den Braber, T. Dimitrakos, R. Fredriken, B. A. Gran, S. hilde Houmb, M. S. Lund, Y. C. Stamatio, and J. O. Aagedal, "Model-based risk assessment: The coras approach," in *Citeseer*, 2002.

[42] H. van der Haar and R. von Solms, "A model for deriving information security control attribute profiles," *Computers & Security*, vol. 22, no. 3, pp. 233 – 244, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404803003110

[43] A. Kankanhalli, H.-H. Teo, B. C. Tan, and K.-K. Wei, "An integrative study of information systems security effectiveness," *International Journal of Information Management*, vol. 23, no. 2, pp. 139 – 154, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401202001056

[44] D. W. Straub and R. J. Welke, "Coping with systems risk: Security planning models for management decision making," *MIS Q.*, vol. 22, no. 4, pp. 441–469, Dec. 1998. [Online]. Available: http://dx.doi.org/10.2307/249551

[45] J. Allen, "Mastering the risk/reward equation: Optimizing information risks to maximize business innovation rewards," RSA, USA, Industry Report, 2008.

[46] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Applied Soft Computing*, vol. 11, no. 7, pp. 4332 – 4340, 2011, soft Computing for Information System Security. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1568494610001419

[47] H. Armstrong, "Managing information security in healthcare - an action research experience," in *Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2000, pp. 19–28. [Online]. Available: http://dl.acm.org/citation.cfm?id=647183.719513

[48] S. A. Butler and P. Fischbeck, "Multi-attribute risk assessment," Proceedings of SREIS, Tech. Rep., 2001.

[49] L. Sun, R. P. Srivastava, and T. J. Mock, "An information systems security risk assessment model under the dempster-shafer theory of belief functions," *J. Manage. Inf. Syst.*, vol. 22, no. 4, pp. 109–142, Apr. 2006. [Online]. Available: http://dx.doi.org/10.2753/MIS0742-1222220405

[50] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 2006, p. 8 pp.

[51] ISO, *Information Technology- Security techniques- Code of practice for information security managment*, ISO/IEC Std. 27 002, 2005.

[52] G. Hardy and E. Guldentops, "Cobit 4.0: The new face of cobit," *Information Systems Control Journal*, vol. 6, pp. 1–36, 2005.

[53] C. J. Alberts and A. J. Dorofee, "Octave sm criteria," Carnegie Mellon University,Software Engineering, Tech. Rep., 2001.

[54] EBIOS, "Ebios : Expression of needs and identification of security objectives." 2004. [Online]. Available: http://www.ssi.gouv.fr

[55] IRAM, "Iram risk assessment process," Internet, 2008, 22 Dec 2010. [Online]. Available: https://www.securityforum.org/services/publictools/publiciram/

[56] A. Asosheh, B. Dehmoubed, and A. Khani, "A new quantitative approach for information security risk assessment," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 2009, pp. 222–227.

[57] E. Kiesling, C. Strausss, and C. Stummer, "A multi-objective decision support framework for simulation-based security control selection," in *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, a, Ed., 2012, pp. 454–462.

[58] K. J. Soo Hoo, "How much is enough: A risk management approach to computer security," Ph.D. dissertation, 2000, copyright - Copyright UMI - Dissertations Publishing 2000; Last updated - 2010-08-07; First page - n/a; M3: Ph.D. [Online]. Available: http://eserv.uum.edu.my/docview/304627006?accountid=42599

[59] A. Jrgenson and J. Willemson, "Processing multi-parameter attacktrees with estimated parameter values," in *Proceedings of the Security 2nd international conference on Advances in information and computer security*, ser. IWSEC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 308–319. [Online]. Available: http://dl.acm.org/citation.cfm?id=1778902.1778930

[60] J. J. Ryan, T. A. Mazzuchi, D. J. Ryan, J. L. de la Cruz, and R. Cooke, "Quantifying information security risks using expert judgment elicitation," *Computers and Operations Research*, vol. 39, no. 4, pp. 774 – 784, 2012, special Issue on Operational Research in Risk Management. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0305054810002893

[61] E. Piatyszek and G. Karagiannis, "A model-based approach for a systematic risk analysis of local flood emergency operation plans: A first step toward a decision support system," *Natural Hazards*, vol. 61, pp. 1443–1462, 2012, 10.1007/s11069-011-0079-z. [Online]. Available: http://dx.doi.org/10.1007/s11069-011-0079-z

[62] M. S. B. Mahmoud, N. Larrieu, and A. Pirovano, "A risk propagation based quantitative assessment methodology for network security - aeronautical network case study," in *Network and Information Systems Security (SAR-SSI)*. La Rochelle, France: IEEE, 2011, pp. 1–9.

[63] G. Koschorreck, "Automated audit of compliance and security controls," in *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on*, may 2011, pp. 137 –148.

[64] A. R. Otero, C. E. Otero, and A. Qureshi, "A multi criteria evaluation of information security controls using boolean features," *Network Security and Its Applications (IJNSA)*, vol. 2, no. 4, pp. 1–11, October 2010.

[65] D. W. Hubbard, *The Failure of Risk Management : Why It is Broken and How to Fix It*, J. Wiley, Ed. New Jeresy,USA: Willy, 2009.

[66] C. Yu and X. Bi, "Survival analysis on information technology adoption of chinese enterprises," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, 2008, pp. 1–5.

[67] C. Otero, E. Dell, A. Qureshi, and L. Otero, "A quality-based requirement prioritization framework using binary inputs," in *Mathematical/Analytical Modelling and Computer Simulation (AMS), 2010 Fourth Asia International Conference on*, 2010, pp. 187–192.

[68] G. Samy, R. Ahmad, and Z. Ismail, "A framework for integrated risk management process using survival analysis approach in information security," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, aug. 2010, pp. 185 –190.

[69] B. von Solms, "Information security governance: Cobit or iso17799 or both?" *Computers & Security*, vol. 24, no. 2, pp. 99 – 104, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404805000210

[70] J. Stevens, R. A. Caralli, and B. J. Willke, "Information asset profiling," Defense Technical Information Center(DTIC), Tech. Rep., 2005.

[71] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Commun. ACM*, vol. 48, no. 2, pp. 78–83, Feb. 2005. [Online]. Available: http://doi.acm.org/10.1145/1042091.1042094

[72] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (rosi): A practical quantitative model," *Journal of Research and Practice in Information Technology*, vol. 38, pp. 45–56, 2006.

[73] R. Matulevicius, N. Mayer, and P. Heymans, "Alignment of misuse cases with security risk management," in *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, ser. ARES '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 1397–1404. [Online]. Available: http://dx.doi.org/10.1109/ARES.2008.88

[74] ENISA, "Risk management: Implementation principles and inventories for risk management and risk assessment methods and tools," ENISA, Paris,France, Technical Report 18062006, June 2006.

[75] A. Tarantino, *Governance, Risk, And Compliance Handbook*, A. Tarantino, Ed. John Wiley and Sons, Inc., 2008.

[76] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," Carnegie Mellon University, Pittsburgh,USA, TECHNICAL REPORT 15213-3890, August 2003.

[77] IRAM. (2011, June) Iram:control selection. https://www.securityforum.org/. InformatinSecurity Forum. [Online]. Available: https://www.securityforum.org

[78] R. Baskerville, "Information systems security design methods: Implications for information systems development," *ACM Comput. Surv.*, vol. 25, no. 4, pp. 375–414, Dec. 1993. [Online]. Available: http://doi.acm.org/10.1145/162124.162127

[79] K. shing Hong, Y.-P. Chi, L. R. Chi, and J.-H. Tang, "An integrated system theory of information security management," *Information Management & Computer Security*, vol. 11, pp. 243–248, 2003.

[80] E. Humphreys, "Information security management standards: Compliance, governance and risk management," XiSEC, Suffolk, Tech. Rep., November 2008, pages 247-255.

[81] R. C. Reid and S. A. Floyd, "Extending the risk analysis model to include market-insurance," *Computers & Security*, vol. 20, no. 4, pp. 331 – 339, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404801004114

[82] R. A. Weber, *Information Systems Control and Audit*, 1st ed. Pearson Education, 1998.

[83] S. Senft and F. Gallegos, *Information Technology Control and Audit, Third Edition*, 3rd ed. Boston, MA, USA: Auerbach Publications, 2008.

[84] T. A. Zia, "An analytical study of it security governance and its adoption on australian organisations," in *Security Research Centre Conferences*, 2010.

[85] A. L. Nnolim, "A framework and methodology for information security management," Ph.D. dissertation, University at Buffalo, 2007.

[86] G. A. Stout, "Improving the decision making process for information security through a pre-implementation impact review of security countermeasures," Ph.D. dissertation, Nova Southeastern University, 2006.

[87] B. Blakley, E. McDermott, and D. Geer, "Information security and risk management," *Communications of the ACM*, vol. 51, pp. 64–68, 2008.

[88] G. Zhi and W. ShengYuan, "Survey of information security risk assessment," in *International Conference on Electrical and Control Engineering*, 2010.

[89] L. Dong-liang and Y. Shi-song, "An information system security risk assessment model based on fuzzy analytic hierarchy process," in *E-Business and Information System Security, 2009. EBISS '09. International Conference on*, may 2009, pp. 1 –4.

[90] UWS, "Hazard identification, risk assessment and control procedure," University of western sydeny, Tech. Rep., 2003.

[91] W. Qiangmin, L. Mengquan, and L. Jianhua, "Method on network information system security assessment based on rough set," in *SITIS '07. Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*. IEEE, 2007, pp. 1041–1046.

[92] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 29 2010-july 1 2010, pp. 1328 –1334.

[93] D. Feng, Y. Zhang, and Y. Zhang, "Survey of information security risk assessment," *China Institute of Communication*, vol. 25, pp. 10–18, 2004.

[94] Z. I. Saleh, H. Refai, and A. Mashhour, "Proposed framework for security risk assessment," *Information Security, 2011*, vol. 2, pp. 85–90, 2011.

[95] V. K. Krishnan, "Efficient processing of system scenarios in statistical and machine learning studies for power system operational and investment planning," Ph.D. dissertation, Iowa State University, 2010.

[96] Y. Zhuang, X. Li, B. Xu, and B. Zhou, "Information security risk assessment based on artificial immune danger theory," in *Computing in the Global Information Technology, 2009. ICCGI '09. Fourth International Multi-Conference on*, aug. 2009, pp. 169 –174.

[97] S. Kondakci, "A causal model for information security risk assessment," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, aug. 2010, pp. 143 –148.

[98] D. V. Bernardo, B. B. Chua, and D. Hoang, "Quantitative security risk assessment (sra) method: An empirical case study," in *World congress on Nature and Biologically Inspired Computing*, Coimbatore, India, 2009, pp. 972–977.

[99] S. Fenz, "An ontology and bayesian-based approach for determining threat probabilities," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 344–354. [Online]. Available: http://doi.acm.org/10.1145/1966913.1966958

[100] J. A. Jones, "An introduction to factor analysis of information risk (fair)," *Norwich Journal of Information Assurance*, vol. 2, p. 67, 2006.

[101] R. Ross, *Security and Privacy Controls for Federal Information Systems and Organizations*, U.S. Department of Commerce Report NIST Special Publication 800-53, 2011.

[102] I. Mkpong-Ruffin, "Quantitave risk assessment model for software in the design phase of software development," Ph.D. dissertation, Auburn University, 2009.

[103] L. Barnard and R. von Solms, "A formalized approach to the effective selection and evaluation of information security controls," *Computers & Security*, vol. 19, no. 2, pp. 185 – 194, 2000. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404800878293

[104] T. Llanso, "Ciam: A data-driven approach for selecting and prioritizing security controls," in *Systems Conference (SysCon), 2012 IEEE International*, 2012, pp. 1–8.

[105] J. Hosey and R. Gamble, "Extracting security control requirements," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW '10. New York, NY, USA: ACM, 2010, pp. 44:1–44:4. [Online]. Available: http://doi.acm.org/10.1145/1852666.1852715

[106] W. A. Al-Hamdani, "Non risk assessment information security assurance model," in *2009 Information Security Curriculum Development Conference*, ser. InfoSecCD '09. New York, NY, USA: ACM, 2009, pp. 84–90. [Online]. Available: http://doi.acm.org/10.1145/1940976.1940993

[107] A. Singh and D. Lilja, "Starts: A decision support architecture for dynamic security configuration management," in *Industrial Engineering and Engineering Management, 2009. IEEM 2009. IEEE International Conference on*, dec. 2009, pp. 2185 –2191.

[108] S. Bandopadhyay, A. Sengupta, and C. Mazumdar, "A quantitative methodology for information security control gap analysis," in *Proceedings of the 2011 International Conference on Communication, Computing*. Rourkela, Odisha, India: ACM, February 2011, pp. 537–540.

[109] F. M. Idris, "E-government technical security controls taxonomy for information assurance contractors: A relational approach," Ph.D. dissertation, University of Maryland, Maryland, 2010, pages 120.

[110] C. Davis, M. Schiller, and K. Wheeler, *IT auditing: Using Controls to Protect Information Assets*, M. Cox, M. Curry, and V. Mehra, Eds. McGraw-Hill Osborne Media, 2006.

[111] V. Verendel, "Quantified security is a weak hypothesis: A critical survey of results and assumptions," in *workshop on New security paradigms workshop*. Oxford, United Kingdom: ACM, 2009, pp. 37–50.

[112] S. A. Butler, "Security attribute evaluation method: a cost-benefit approach," in *Proceedings of the 24rd International Conference on Software Engineering,ICSE 2002*, 2002.

[113] D.-M. Zhao, J.-H. Wang, and J.-F. Ma, "Fuzzy risk assessment of the network security," in *International Conference on Machine Learning and Cybernetics*, 2006.

[114] R. Cambra, "Metrics for operational security control," SANS, Tech. Rep., 2004.

[115] E. A. Fischer, "Creating a national framework for cybersecurity: An analysis of issues and options," Science and Technology Resources, Science, and Industry Division, The Library of Congress, Tech. Rep. RL32777, February 2005.

[116] ISO, *Information Technology- Security techniques- Information security management system- requirements*, ISO/IEC Std. 27 002, 2005.

[117] J. Hagerty, K. Verma, and D. Gaughan, "The governance, risk management, and compliance (grc) landscape," AMR, Boston,USA,, Tech. Rep., 2008.

[118] G. Chacko, P. Tufano, and G. Verter, "Taking risk management theory seriously," *Journal of Financial Economics*, vol. 60, pp. 449 – 485, 2001, complementary Research Methodologies: The InterPlay of Theoretical, Empirical and Field-Based Research in Finance. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0304405X01000502

[119] S. R. Ashmore, M. Castillo, and B. Gavric, *Guide for Assessing the Security Controls in Federal Information Systems*, NIST Std., 2008.

[120] V. Vidutoa, C. Maplea, W. Huanga, and D. Lopez-Perezb, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," *Decision Support Systems*, vol. 1, p. 37, 2012.

[121] A. Singh and D. J. Lilja, "Criteria and methodology for grc platform selection," *ISACA (Information System Audit and Control Association) Journal*, vol. 1, p. 6, 2010.

[122] C. Woody, "Applying octave:practitioners report," Carnegie Mellon University, Tech. Rep. CMU/SEI-2006-TN-010, 2006.

[123] C. J. Alberts, A. J. Dorofee, and J. H. Allen, "Octave sm catalog of practices," Carnegie Mellon University,Software Engineering, Technical Report, 2001.

[124] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, L. Pesante, Ed. New York: Addison-Wesley Professional, 2009.

[125] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro:improving the information security risk assessment process," Carnegie Mellon University, Pittsburgh,USA, Tech. Rep., 2007.

[126] A. Otero, G. Tejay, L. Otero, and A. Ruiz-Torres, "A fuzzy logic-based information security control assessment for organizations," in *Open Systems (ICOS), 2012 IEEE Conference on*, 2012, pp. 1–6.

[127] P. Bilski, "An unsupervised learning method for comparing the quality of the soft computing algorithms in analog systems diagnostics," in *Mixed Design of Integrated Circuits Systems, 2009. MIXDES '09. MIXDES-16th International Conference*, june 2009, pp. 499 –504.

[128] A. H. Phyo and S. M. Furnell, "A detection-oriented classification of insider it misuse," in *in Third Security Conference*, 2004.

[129] CRIMM. (2011) Cramm. CRAMM. http://www.cramm.com/. [Online]. Available: http://www.cramm.com/

[130] R. Plackett and J. Burman, "The design of optimum multifactorial experiments," *Biometrika*, vol. 33, pp. 305–325, 1946.

[131] J.-J. Lv, Y.-S. Zhou, and Y.-Z. Wang, "A multi-criteria evaluation method of information security controls," in *Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on*, 2011, pp. 190–194.

[132] H. Ogut, "Information technology security risk management," Ph.D. dissertation, The University of Texas at Dallas, 2006.

[133] M. Krey, "Information technology governance, risk and compliance in health care - a management approach," in *Developments in E-systems Engineering (DESE)*, 2010, pp. 7–11.

[134] L. T. M. Blessing and A. Chakrabarti, *DRM, a Design Research Methodology*, 1st ed., Springer, Ed. Springer Publishing Company, Incorporated, 2009.

[135] A. Habbal, "Tcp sintok: Transmission control protocol with delay-based loss detection and contention avoidance mechanisms for mobile ad hoc networks," Networked Computing, School of Computing, Universiti Utara Malaysia, 2014.

[136] S. Fenz and A. Ekelhart, "Verification, validation, and evaluation in information security risk management," *IEEE Security and Privacy*, vol. 9, no. 2, pp. 58–65, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1109/MSP.2010.117

[137] M. S. Feather, S. E. Cornford, K. A. Hicks, and K. R. Johnson, "Applications of tool support for risk-informed requirements reasoning," *International Journal of Computer Systems Science & Engineering*, vol. 20, no. 1, pp. 5–18, 2005.

[138] G. Dhillon and G. Torkzadeh, "Value-focused assessment of information system security in organizations," *Information Systems Journal*, vol. 16, no. 3, pp. 293–314, 2006. [Online]. Available: http://dx.doi.org/10.1111/j.1365-2575.2006.00219.x

[139] N. Feng and J. Xie, "A hybrid approach of evidence theory and rough sets for iss risk assessment," *JOURNAL OF NETWORKS*, vol. 7, p. 8, 2012.

[140] Nessus, "Nessus," http://www.tenable.com/products/nessus/select-your-operating-system, 2014.

[141] Nmap, "Nmap tool," http://nmap.org/, 2014.

[142] Netstumbler, "Wi-fi security," http://www.netstumbler.com/, 2013.

[143] Wireshark, "Wireshark," http://www.wireshark.org/about.html, 2013.

[144] kismet, "Kismet wireless," https://www.kismetwireless.net/, 2014.

[145] Metasploit, "Metasploit tool," http://www.metasploit.com/, 2013.

[146] Airsnort, "Airsnort advanced tool," http://airsnort.shmoo.com/, 2012.

[147] N-Stealth, "N-stealth http security scanner," http://www.securityfocus.com/tools/2109, 2013.

[148] ACUNETIX. (2006) Acunetix web vulnerability scanner. https://www.cccure.org/Documents/acunetix/acunetix.pdf.

[149] C. Kahraman and S. Ceb, "A new multi-attribute decision making method: Hierarchical fuzzy axiomatic design," *Expert Syst Appl.*, vol. 36, no. 3, pp. 4848–4861, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.eswa.2008.05.041

[150] E. K. Zavadskas, A. Kaklauskas, Z. Turskis, and J. Tamošaitienė, "Multi-attribute decision-making model by applying grey numbers," *Informatica*, vol. 20, no. 2, pp. 305–320, Apr. 2009. [Online]. Available: http://dl.acm.org/citation.cfm?id=1576292.1576302

[151] A. S. B. Inglesant, "Trust economics: A systematic approach to information security decision-making," Dept. of Computer Science in University College London, Tech. Rep., 2010.

[152] C. Hwang and K. Yoon, *Multiple Attribute Decision Making Methods and Applications: A State-of-the Art Survey*, ser. Lecture Notes in Economics and Mathematical Systems Series. Springer London, Limited, 1981. [Online]. Available: http://books.google.com.my/books?id=4Z67QgAACAAJ

[153] K. P. Yoon and C. L. Hwang, *Multiple Attribute Decision Making: An Introduction (Quantitative Applications in the Social Sciences*. USA, SAGE Publications, Inc., 1995, vol. 104:83.

[154] S.-Y. Chou, Y.-H. Chang, and C.-Y. Shen, "A fuzzy simple additive weighting system under group decision-making for facility location selection with objective or subjective attributes," *European Journal of Operational Research*, vol. 189, no. 1, pp. 132 – 145, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0377221707004754

[155] H.-S. Shih, H.-J. Shyur, and E. S. Lee, "An extension of topsis for group decision making," *Mathematical and Computer Modelling*, vol. 45, pp. 801 – 813, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0895717706003025

[156] Y.-H. Chang and C.-H. Yeh, "Evaluating airline competitiveness using multiattribute decision making," *Omega*, vol. 29, no. 5, pp. 405 – 415, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0305048301000329

[157] S. Opricovic and G.-H. Tzeng, "Compromise solution by mcdm methods: A comparative analysis of vikor and topsis," *European Journal of Operational Research*, vol. 156, no. 2, pp. 445 – 455, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0377221703000201

[158] G. H. Tzeng and J.-J. Huang, *Multiple Attribute Decision Making: Methods and Applications*, C. Press, Ed. CRC Press, 2011.

[159] F. T. Sheldon and R. K. Abercrombie, "Methodology for evaluating security controls based on key performance indicators and stakeholder mission," in *Proceedings of the 42nd Hawaii International Conference on System Sciences*, ser. HICSS '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 1–10. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2009.308

[160] D. J. Lilja, *Measuring Computer Performance*, C. University, Ed. Cambridge University Press United Kingdom, 2000.

[161] A. B. Knol, P. Slottje, J. P. van der Sluijs, and E. Lebret, "The use of expert elicitation in environmental health impact assessment: a seven step procedure," *Environmental Health*, vol. 9, no. 1, p. 19, 2010.