Risk Management in Information Security: A Systematic Review

Manuel Alcántara
Maestría en Informática, Escuela de Posgrado, Pontificia Universidad Católica del Perú, Lima, Perú
Email: malcantarar@pucp.pe

Andrés Melgar
Grupo de Reconocimiento de Patrones e Inteligencia Artificial Aplicada, Sección de Ingeniería Informática, Departamento de Ingeniería, Pontificia Universidad Católica del Perú, Lima, Perú
Email: amelgar@pucp.edu.pe

***Abstract*—The risks of information assets have complex nature; the management of risk of information security is addressed by different approaches. The aim of this work is to establish the state of the art in the management of risk of information security. To achieve this purpose we conducted a Systematic Review of the literature in the main bibliographic databases. It determined that there are several studies about the methods, exist different approaches about the risk analysis including the Artificial Intelligence. There are studies about the aligning of business plans with the aspects of information security but little information about the results his implementation, maturity and simulation of controls. It should investigate more about these shortcomings.**

***Index Terms*—information assets, state of art, risk analysis, risk assessment**

I. Introduction

Due to the increase of mobile computing, cloud computing services and the use of social networks, the information is more and more in risk. Information Security (IS) studies the preservation of integrity, confidentiality and availability of information assets [1]. To manage information asset risks, Information Security Management System (ISMS) have been implemented. This kind of system has an important component, the management the Risks of Information Security (RIS). The Management the Risks of Information Security (MRIS) comprising i) identification of RIS, external events that could have a negative impact on information assets; ii) analysis of RIS, the cataloging, understanding and appreciation of the issues related to RIS; iii) treatment of RIS, lead to the development of a risk treatment plan, where RSI management criteria are defined; iv) implementation of controls, a set of safeguards grouped by projects, both organizational and management, and implementation of technological measures; and v) monitoring and control of RIS, It consists in evaluating the existence and proper functioning of the system of integrated Risk Management (RM) [2], [3].

In this work we try to identify and analyze systematically the research about the management of RIS published in major bibliographic databases. Interested to know what the state of the art, know what are the existing methodologies, the efficiency and effectiveness of these methods, how to assesses these kind of systems, the successful cases in the methodologies implementation, how the implemented controls have matured, the adjustments for cloud computing, the use of strategies and techniques unconventional as Artificial Intelligence. To achieve this objective was used the literature search strategy called Systematic Review (SR). It is the implementation of a detailed and systematic process where is defined the form of conducting the search for papers published in major bibliographic databases of the world recognized and accepted by the scientific community.

This paper was structured in four sections. At first is presented the introduction. Secondly, it is presented the materials and methods. In the section three is detailed and discussed the systematic review performed. Finally, in the section four is discussed some relevant points and addressed future works.

II. Systematic Review

Systematic Review (SR) is a method of bibliographic research for evaluates and analyzes the research that exists about a particular topic or an area of interest in reliable sources of scientific information [4], [5]. In contrast to a conventional literature review, a SR follows a strict and well-structured sequence of methodological steps, which ensure a high scientific value of the results. This methodological structure allows the review can be repeated for any researcher interested in the issue by following the steps set. Consists of three main blocks of activities: i) planning review, ii) conducting the review; and iii) reporting the review. When planning SR, the purpose and scope of the work is defined. The purpose of the investigation is clearly established through the research questions, which are associated with the objectives of the SR. When conducting the SR, a critical

Manuscript received August 25, 2015; revised November 11, 2015.

doi: 10.12720/jait.7.1.1-7

analysis of selected works is done in order to answer the research questions.

Based on preliminaries studies, we posed the six research questions (see Table I). These research questions guided the design of the review process. Studies dealing with RM in general, that deal with the management of other risks not considered technical and gray information were not analyzed (exclusion criteria). The empirical studies were identified from the Science Direct, ACM Digital Library, IEEE Xplore Digital Library, SCOPUS, Google Scholar, ProQuest, EBSCO databases.

TABLE I. MAIN MOTIVATIONS AND RESEARCH QUESTIONS

Main motivation	Research question
Determine and analyze scientific studies about the methodologies for the MRIS	RQ1: What are the methodologies and methods to manage RIS?
Identify studies about analysis of RIS	RQ2: How the analysis of RIS is done?
Identify and analyze the efficiency and effectiveness of MRIS	RQ3: How the efficiency and effectiveness of MRIS is measured?
Identify research dealing with the use of Artificial Intelligence in MRIS	RQ4: Are the MRISs addressed by Artificial Intelligence?
Identify and analyze research dealing about maturity of controls in MRIS	RQ5: How maturity of controls for the RIS is addressed?
Identify and analyze studies that treat adaptations of controls of MRIS to Cloud Computing	RQ6: Are the criteria for MRIS appropriate for cloud computing?

The search was performed on March 2015. The search strings used are showed in the Table II, we perform one search for each research question. After reviewing the abstract, introduction and conclusions of the studies, the content was analyzed and finally were selected the articles that answer the respective research questions. The studies were categorized in eleven topics in order to organize the studies for each question. A total of 70 studies were analyzed.

TABLE II. SEARCH STRINGS FOR RESEARCH QUESTIONS

	Search strings	Topic	Quantity
RQ1	((risk management information security) AND (method OR methodology OR process))	Methods	16
RQ2	(risk information security assessment)	Evaluation	17
RQ3	((risk management information security) AND (effectiveness OR efficiency OR metric OR reliability OR satisfaction))	Effectiveness	3
		Efficiency	4
RQ4	((risk management information security) AND (neural network OR genetic algorithm OR fuzzy logic OR bayesian networks OR ontologies))	Neural networks	4
		Genetic Algorithms	4
		Fuzzy logic	10
		Bayesian networks	3
		Ontologies	3
RQ5	((risk management information security) AND (maturity OR control))	Maturity	3
RQ6	((risk management information security) AND (cloud computing))	Cloud Computing	3

III. RESULTS AND DISCUSSION

A. Methods for Managing RIS

ISO 27005:2008. Establishes guidelines for the MRIS. It is the complement of the ISO/IEC 27001 and ISO/IEC 27002 standards, which define the need to manage the RIS, without specifying how. It is perceived as formalizing international requirements to be met by a methodology of MRIS. The critics of this standard do not see a real contribution in it. Criticism focuses on that the new standard not delves really into MRIS, it is merely a declarative framework. Regardless of the controversies, this standard has generally served as a reference and inspiration for the proposed and formulation of others methods for the treatment of RIS [6].

MAGERIT. It is an open methodology with widespread use in the Spanish context and mandatory for use in Spanish public administration. It is structured into three parts: method, catalog of elements and technical guide [7].

OCTAVE. Focuses on the study of organizational risks, mainly in aspects related to every day work in organizations [8], [9]. One of its peculiarities is that it must be performed by personnel belonging functional units and information technology area. There are: OCTAVE (for large organizations), OCTAVE-S (for small organizations) and OCTAVE Allegro (defined to analyze risks with a greater focus on information assets, as opposed to the approach in information resources).

CRAMM. It is implemented in three phases: i) establishment of security objectives, ii) risk assessment; and iii) identification and selection of counter-measures. It is applicable to all kinds of information systems and can be used in all stages of the life cycle. Provides a tool that supports it, which a database of more than 400 types of assets, more than 25 types of impacts, 38 types of threats, 7 types of risk measures and more than 3,500 safeguards [6], [10].

EBIOS. Provides a comprehensive methodological approach in accordance with the main international RM standards. Establishes a baseline for the certification of competencies related to RM and is applicable to both the public and private sectors, small medium and large enterprises in francophone countries [11].

IT Baseline Protection Manual. Interprets the general proposals of the family ISO 27000 and helps users to implement them in practice with many notes, examples and background knowledge [11].

NIST SP 800-30. It is part of the SP800 series dedicated to IS and published by National Institute of Standards and Technology. This series includes a methodology for the analysis and MRIS aligned [6], [10].

ARIMA. Covers more fully the processes of ISO/IEC 27005 not covered with methodologies like CRAMM, EBIOS, OCTAVE. The core is to combine the advantages of such methodologies, leveraging the proven techniques and adapt them to comply with the MRIS process [1].

MEHARI. Developed for help managers to do MRIS and reduce the associated risks. Reducing risk involves a

prior knowledge of management strategies and business processes in order to optimize the investments in security measures both technical and organizational [7].

Microsoft's Security Management Guide. Establishes a formal process for the MRIS, allowing companies to operate in the most effective manner with an acceptable level of risk [12].

CORAS. It is a method for MRIS using primarily the interviews with experts. It uses i) the UML for defining models for assets, threats, risks, safeguards; ii) a graphical editor based on Microsoft Visio; iii) a library of reusable cases and iv) a textual representation of graphic language based on XML [13].

COBIT. It is a framework for the management of Information Technology (IT), as well as support tools that allows to bridge the gap between control requirements, technical issues and business risks. In relation to IS and in particular the management of RIS, COBIT contains a framework called Risk IT consisting of a set of guiding principles for MRIS, Risk IT complements [14], [15].

ISM3. It is a management methodology of maturity of controls of MRIS. It is aligned with quality management ISO 9001 and applied to the ISMS. It establishes different levels associated with the controls in MRIS [16]. The aim is to provide best practices to achieve the highest level. It complies with the requirements of ISO/IEC 27001 and presents other methods [3].

B. Evaluation of RIS

Quantitative methodologies. Reference [17] adopts data mining to find the relationship between asset and threat-vulnerability, and propose a method identifying threat and vulnerability. Reference [18] presents a RIS method that considers risk elements, like asset dependency, vulnerability dependency, etc. during risk computation. Reference [19] combines Analytic Hierarchy Process (AHP) and Group Decision Making (GDM) methods for propose a new method for MRIS. AHP is a technique to generate models for structured problems of making decisions. It is now used as a technique to support other problems of unstructured nature. GDM is a participatory process in which multiple individuals acting collectively to analyzing problems and proposing solutions. Reference [20] presents an approach based on AHP and Formal Safety Assessment (FSA) for MRIS. FSA is a methodology, aimed at assessing the risk related to maritime safety and the protection of the marine environment. Reference [21] proposes a MRIS method that considers both the enterprise objectives and the scalability in the Attack tree (AT) model. Reference [22] uses the Fault Tree Model for MRIS. They analyze the risk and his probability and calculate the risk structure overall of the system and the main faults which can be quantitatively analyzed, they establish methods to diagnose faults and how to treat them. Reference [23] uses Danger Theory (DT) for immunology to propose a DT model for the MRIS, consider the correlation between the evaluation factors to determine the dynamic assessment of changes of the risk. Reference [3] presents a method for MRIS based on the models Callio Secura (CS) and Microsoft Assessment (MS).

Qualitative methodologies. Reference [24] has made several proposals for qualitative analysis as AHP, Neural Networks (NN), fuzzy theory, among others, which use mathematical and statistical tools. Reference [25] discusses the relationship between the concepts and processes for MRIS, based on the operations and the way of organization of the institution. They conclude that these two processes cannot be conceived separately, they show that both efforts respond to the same goal. Reference [26] outlines how a RIS assessment method can be elaborated using knowledge-centric analysis of information assets, suggest the use of a genre-based analysis method for identifying organizational communication patterns, through which organizational knowledge is shared.

Hybrid methodologies. Reference [27] proposes a hybrid procedure for evaluating RIS. They suggest the use of 17 groups of controls proposed by the NIST. First, they use Decision Making Trial Evaluation Laboratory to obtain a map of relationships between controls, secondly; they use Analytic Network Process to obtain a classification of the risk obtaining quantitative data. For the qualitative part they suggest using expert opinion and professionals. In [28], AHP was used for MRIS to realize the transformation from qualitative analysis to quantitative analysis getting the weight of risk factors and uses PDCA (Plan-Do-Check-Action) cycle method..

Successful cases. Reference [29] presents the results after the implementation of a MRIS for small organizations based on OCTAVE-Small. Reference [30] presents an implementation of MRIS in a system video call from mobile phones in medical emergencies. Reference [31] shows the implementation of MRIS in the manufacturing industry in China. Reference [32] does the guidelines of a Business Continuity Plan for e-government in China. Reference [33] presents a method adapted for MRIS for public organizations in Turkey. Reference [34] exhibits the implementation of a system of MRIS for a Hospital Pediatric Italian based on ISO/IEC 27002. Reference [35] makes a study on the security risks in RFID based on the recommendations of ISO 27001.

C. Efficiency and Effectiveness of Controls

Boehmer [36] affirms that the study of efficiency and effectiveness in the MRIS is related to the efficiency and effectiveness of the ISMS, also asserts that both are not addressed by most for MRIS methodologies, and that MRIS are generally understood in terms of quality and are therefore described by COBIT without specifying how they should be measured. The measurement of the efficiency and effectiveness of controls should be done under the concept of organizational value chain. Reference [12] argues that efficient in MRSI is the ability to establish the proper alignment between the cost of implementation and the real risk that the organization must assume. Reference [37] proposes a method for the selection of the optimal investment in IS based in quantifying system protection values and defines metrics to measure the risk. Reference [38] makes a study of the effectiveness of MRIS by relating the investment in

MRIS versus the losses that occurred because of safety incidents. Describes a model for determines the optimal amount to invest in IS. Reference [39] presents a holistic approach to implement or upgrade ISMS. They propose meta-processes and present the specifications that should have a virtual platform for sharing.

D. Artificial Intelligence and MRIS

Neural networks. Reference [40] proposes a model for MRIS, based on one type of NN. Zhao [41] applied the theory of statistical learning (SLT) of NN. It establishes the usefulness of applying this theory to solve the complicated problems of the MRIS. It claims that is effective the application of SLT to defend of the imprecise and potential risks, and is also effective for automatic reduction of the magnitude of security incidents. Reference [42] proposed a method for MRIS which combines wavelet NN (WNN) and the of entropy-grey correlation, they do the comparisons between WNN and other traditional estimation methods in terms of convergent speed, training precision and forecasting effect. Reference [43] combines the theory of WNN and Fuzzy Logic (FL). It concludes that the uncertainty in the MRIS and the subjectivity of the assessment can be reduced by using this technique.

Genetic algorithms. Reference [44] presents a system for the MRIS by using Genetic Algorithms (GA) to search for rules identifying risks based on historical data. It develops a Bayesian network (BN) to predict the risks by identifying its origin to establish appropriate measures and reduce the probability of risk. Reference [45] proposes a method for risk detection, based on optimization GA-Chaos and NN RBF. Chaos is a common nonlinear phenomenon in nature, having intrinsic random properties and implicit rules. Optimization GA-Chaos combines the chaotic search properties with the parameters to be optimized. It encoding the chaotic variables, which are represented as chromosomes, does the chaotic intersection and the chaotic mutation according to the principle of survival of the fitness. The GA-Chaos was first used to optimize the structure and its weights for higher learning and generalization ability of the RBF model detected. The RBF model was then used to train and test data-sets intrusion. Reference [46] proposes a multi- objective GA that was used as an optimization technique capable of finding optimal solutions. The result of the optimization routine is a set of solutions, the final decision can be implemented to reduce risk and meet a certain budget. Tamjidyamcholo [47] apply a GA for reducing the uncertainty of RIS.

Bayesian networks. Reference [48] presents a BN for the treatment of RIS, uses probabilistic reasoning to find the value of the risk and combined with expert knowledge previously stored. Reference [49] proposes a model for RIS assessment based on observed cases and the domain experts. A GA is applied to find the rules for identification of RIS based on historical data. To identify the causal relationships of risk factors and predict the probability of RIS, a BN is developed. Reference [50] presents an approach; where Dynamic BN models are constructed to identify multi stage attacks. The Dynamic BN models help to detect the uncertain relationship associated with the risk event. The next task is inferring, where evidence is updated dynamically for the multiple time slices. Finally, a diagrammatic representation of the attack scenario and the constructed Dynamic BN is shown to explain the effectiveness of the model in identifying multi stage attacks

Fuzzy Logic. Reference [51] adopts fuzzy decision tree to evaluate the information security risk assessment for decision-makers. Reference [52] presents a method for MRIS based on operations with Fuzzy Numbers (FN), Fuzzy linguistic variables and opinions of experts integrated into triangular FN. Reference [13] proposes a method for evaluating the RIS using FL. It quantifies the risk of assets and determines the degree of dependence of the shared information, then gets the optimal points in each level of risk as central points, using the algorithm K-means. Reference [42] presents a mechanism for the generation of RIS, based on the assessment of risk factors; the model for the evaluation of the RIS system is built using the Fuzzy Analytic Hierarchy method. Shameli-Sendi [53] presents a model for the evaluation of RIS. It is based on multiple criteria for decision-making and uses FL, it is proposed as a qualitative approach in accordance with ISO/IEC 27005 considering the business processes both of management and operational levels. Reference [54] proposes a method to integrate multiple levels of assessment Fuzzy Grey for assessing quantitative the RIS. Reference [55] does an improved Fuzzy AHP method based on triangular FN, the calculation model is established. The evaluation of information security systems is made by using a fuzzy integral assessment. Reference [56] uses the FL and the Gray Relational analysis for evaluation of RIS. Reference [57] presents a model for the evaluation of RIS based on DT, they propose and provide a method of calculating the risk based on this model by reference to the dynamic characteristic of the theory of immunology. Reference [58] proposes an approach based on the theories of fuzzy comprehensive judgment. It analyzes the risk factors of the IS such as the system risk, network risk, security management risk, environment risk and operation risk.

Ontologies. Reference [59] discussed how to use ontologies in the construction of knowledge base for the RIS. Reference [60] presents an ontological model for the MRIS. Reference [61] proposes ontology knowledge base construction method for information security, discuss the ontology construction processes.

E. Maturity in MRIS

Reference [62] presents a model with three maturity levels that determine the degree of IS. Reference [63] describes the structure of a model for assessing the maturity level of process of MRIS, aligned with ISO/IEC 27005. Reference [64] presents a framework for the MRIS as a unified platform to address the complex evolution of RIS. They say that given the endemic nature of RIS, the approach requires periodically rethink the MRIS. This approach depends on the maturity level of MRIS controls.

Simulation of controls of RIS. This is not done with conventional methods; however are used algorithms for training and learning NN, unconventional optimization of GA, algorithms of BN. There is a little literature on the simulation of controls for RIS. Boehmer [65] uses game theory (GT) to simulate the route of infection to an alleged attack by viruses.

F. Cloud Computing and RIS

Reference [66] presents a model to adapt to the cloud computing, according the ISO 27000 family of standards. Reference [67] presents a framework for MRIS in the cloud, covering models of services and models of implementation. Reference [68] formulates the implications of Cloud Computing risks on personal health information.

IV. Conclusions

The MRIS is widely treated in several projects, was studied in detail methodologies, analysis of RIS, but there are few studies related to the efficiency, effectiveness and maturity of the controls, which opening possibilities for future research. The complex nature of RIS involves aspects of uncertainty, dynamism and probability which have determined the use of AI techniques such as NN, FL, GA and other such as GT, Bayesian networks, HAP. To achieve a higher level of deployment of cloud computing, it needs to adapt the recommendations of the standards of IS to this new technology. There are few studies on this subject. There is a little evidence for the existence of an integrated approach to the MRIS that considers both the design of the information system for RIS and the analysis of RIS. This need is being addressed as a research by the European project CORAS. There is an urgent need for research to simulate the IS controls before deployment in organizations using such GA or NN. It is recommended research that emphasizes the maturity of controls, RIS within a holistic environment and continuous improvement. Research should be done on ontologies to formulate structures to automate MRIS and developed software tools to support it.

References

[1] A. Leitner, I. Schaumuller-Bichl, and A. Arima, "New approach to implement ISO/IEC 27005," in *Proc. 2nd International Logistics and Industrial Informatics*, Austria, 2009, pp. 1-6.

[2] M. Spremic, "Corporate IT risk management model: A holistic view at managing information system security risks," in *Proc. the International Conference on Information Technology Interfaces*, ITI. Cavtat / Dubrovnik, Croatia, 2012, pp. 299-304.

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

[4] O. Pedreira, M. Piattini, M. R. Luaces, and N. R. Brisaboa, "A systematic review of software process tailoring," *SIGSOFT Softw. Eng. Notes,* vol. 32, no. 3, pp. 1-6, 2007.

[5] P. Mian, T. Conte, A. Natali, J. Biolchini, and G. Travassos, "A systematic review process for software engineering," in *Proc. 2nd Experimental Software Engineering Latin American Workshop*, Brazil, 2005.

[6] A. A. Ekelhart, S. B. Fenz, and T. A. Neubauer, "Aurum: A framework for information security risk management," in *Proc. 42nd Annual Hawaii International Conference on System Sciences, HICSS*, Vienna, Austria, 2009.

[7] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in *Proc. International Conference on Availability, Reliability and Security, ARES*, Fukuoka, Japan, 2009, pp. 726-731.

[8] G. N. Samy, R. Ahmad, and Z. Ismail, "A framework for integrated risk management process using survival analysis approach in information security," in *Proc. 6th International Conference on Information Assurance and Security*, Atlanta, United States, 2010, pp. 185-190.

[9] J. Paulina and D. Marek, "Designing a security policy according to BS 7799 using the OCTAVE methodology," in *Proc. Second International Conference on Availability, Reliability and Security, ARES*, Vienna, Australia, 2007, pp. 715-722.

[10] P. A. Shamala, R. A. Ahmad, and M. C. Yusoff, "A conceptual framework of info structure for information security risk assessment," *Journal of Information Security and Applications*, pp. 45-52, 2013.

[11] H. Elachgar and B. Regragui, "Information security, new approach," in *Proc. 2nd International Conference on Innovative Computing Technology, INTECH 2012*, Morocco, 2012, pp. 51-56.

[12] I. Tashi and S. Ghernaouti-Hélie, "Efficient security measurements and metrics for risk assessment," in *Proc. 3rd International Conference on Internet Monitoring and Protection, ICIMP*, Bucharest, Romania, 2008, pp. 131-138.

[13] G. H. Gao, X. Y. Li, B. J. Zhang, and W. X. Xiao, "Information security risk assessment based on information measure and fuzzy clustering," *Journal of Software*, vol. 6, no. 11, pp. 2159-2166, 2011.

[14] S. Morimoto, "Application of COBIT to security management in information systems development," in *Proc. 4th International Conference on Frontier of Computer Science and Technology*, 2009, pp. 625-630.

[15] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations," in *Proc. Second Asia International Conference on Modeling & Simulation*, Malaysia, 2008, pp. 749-753.

[16] M. S. Salehand and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Applied Computing and Informatics*, vol. 9, no. 2, pp. 107-118, 2011.

[17] Y. C. Chu, Y. C. Wei, and W. H. Chang, "A risk recommendation approach for information security risk assessment," in *Proc. 15th Asia-Pacific Network Operations and Management Symposium: Integrated Management of Network Virtualization*, Taoyuan, Taiwan, 2013, pp. 120-127.

[18] J. Bhattacharjee, A. Sengupta, and C. Mazumdar, "A formal methodology for enterprise information security risk assessment international," in *Proc. Conference on Risks and Security of Internet and Systems*, Kolkata, India, 2013.

[19] Z. H. Xinlan, W. Zhifang, Guangfu, and Z. Xin, "Information security risk assessment methodology research: Group decision making and analytic hierarchy process," in *Proc. 2nd WRI World Congress on Software Engineering, WCSE*. Wuhan, China, 2010, pp. 157-160.

[20] Z. Q. Wei and M. F. Li, "Information security risk assessment model base on FSA and AHP," in *Proc. International Conference on Machine Learning and Cybernetics, ICMLC*, Qingdao, China, 2010, pp. 2252-2255.

[21] B. Karabey and N. Baykal, "Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities," *International Arab Journal of Information Technology*, pp. 297-305, 2013.

[22] H. X. Tao, C. Liang, W. Chi, and H. L. Qun, "The research of information security risk assessment method based on fault tree," in *Proc. International Conference on Networked Computing and Advanced Information Management*, 2010, pp. 370-375.

[23] Y. Zhuang, X. Li, B. Xu, and B. Zhou, "Information security risk assessment based on artificial immune danger theory," in *Proc. 4th International Multi-Conference on Computing in the Global Information Technology, ICCGI*. Cannes, La Bocca, France, 2009, pp. 169-174.

[24] Q. Ye. Qing, C. H. Zhang, X. P. Wu, and D. J. Zhai, "Information security risk assessment based on AHP/DST," in *Proc. International Conference on Management and Service Science*, 2009.
[25] I. Tashi and S. Ghernouti-Hélie, "Information security management is not only risk management," in *Proc. 4th International Conference on Internet Monitoring and Protection, ICIMP*. Venice, Mestre, Italy, 2009, pp. 116-123.
[26] A. M. Padyab, T. Päivärinta, and D. Harnesk, "Genre-based assessment of information and knowledge security risks," *Annual Hawaii International Conference on System Sciences*, Sweden, 2014, pp. 3442-3451.
[27] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Systems with Applications*, vol. 39, no. 1, pp. 247-257, 2012.
[28] M. Meng, "The research and application of the risk evaluation and management of information security based on AHP method and PDCA method," in *Proc. 6th International Conference on Information Management, Innovation Management and Industrial Engineering*, Hainan, China, 2013, pp. 379-383.
[29] M. Moyo, H. Abdullah, and R. C. Nienaber, "Information security risk management in small-scale organizations: A case study of secondary schools computerised information systems," in *Proc. 2013 Information Security for South Africa*, Sandton, Johannesburg, South Africa, 2013.
[30] S. R. Bolle, P. Hasvold, and E. Henriksen, "Video calls from lay bystanders to dispatch centers-Risk assessment of information security," *BMC Health Services Research*, vol. 11, 2011.
[31] W. Dai, Q. Zhu, C. Wang, and Y. Zeng, "Risk management model of information security in IC manufacturing industry," *Journal of Computers*, vol. 7, no. 2, pp. 317-324, 2012.
[32] W. Xiang, Y. Wang, and Z. Zhang, "The research on business continuity planning of E-government based on information security risk management," in *Proc. IEEE International Conference on Networking, Sensing and Control*, Sanya, China, 2008, pp. 446-450.
[33] S. Ozkan and B. Karabacak, "Collaborative risk method for information security management practices: A case context within Turkey," *International Journal of Information Management*, vol. 30, no. 6, pp. 567-572, 2010.
[34] M. Bava, D. Cacciari, E. Sossa, R. Zangrando, and D. Zotti, "Information security risk assessment in healthcare: The experience of an Italian pediatric hospital," in *Proc. 1st International Conference on Computational Intelligence, Communication Systems and Networks*, 2009, pp. 321-326.
[35] F. T. Wang and T. D. Wu, "Information security on RFID based power meter system," in *Proc. 2nd IEEE International Conference on Information Management and Engineering*, 2010, pp. 317-320.
[36] W. Boehmer, "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001," in *Proc. 2nd Int. Conf. Emerging Security Inf., Systems and Technologies, SECURWARE 2008, Includes DEPEND 2008: 1st Int. Workshop on Dependability and Security in Complex and Critical Inf. Sys.* France, 2008, pp. 224-231.
[37] R. Bojanc and B. Jerman-Blažic, "An economic modelling approach to information security risk management," *International Journal of Information Management*, vol. 28, no. 5, pp. 413-422, 2008.
[38] Z. Lu, X. Wang, X. B. Liu, and R. Xu, "Study on efficiency of risk management for information security based on transaction," in *Proc. 2nd International Symposium on Electronic Commerce and Security*, Nanchang, China, 2009, pp. 356-360.
[39] E. Papadaki, D. Polemi, and D. K. Damilos, "A holistic, collaborative, knowledge-sharing approach for information security risk management," in *Proc. the 3rd International Conference on Internet Monitoring and Protection*, Bucharest, Romania, 2008, pp. 125-130.
[40] H. Niu and Y. Shang, "Research on risk assessment model of information security based on particle swarm algorithm -RBF neural network," in *Proc. 2nd Pacific-Asia Conference on Circuits, Communications and System, PACCS 2010*, Beijing, China, 2010, pp. 479-482.
[41] L. Zhao, Y. Wu, and X. Wu, "Research of information security risk management based on statistical learning theory," *International Forum on Computer Science-Technology and Applications*, Chongqing, China, pp. 436-438, 2009.
[42] D. L. Liu and S. S. Yang, "An information system security risk assessment model based on fuzzy analytic hierarchy process," in *Proc. International Conference on E-Business and Information System Security, EBISS*, Wuhan, China, 2009.
[43] D. M. Zhao, J. X. Liu, and Z. H. Zhang, "Method of risk evaluation of information security based on neural networks," in *Proc. International Conference on Machine Learning and Cybernetics*, Baoding, China, 2009, pp. 1127-1132.
[44] N. Feng, J. Xie, and P. Chang, "An intelligent system to assessing information systems security risks in electronic business," in *Proc. the 2012 4th International Symposium on Information Science and Engineering*, Shanghai, China, 2012, pp. 303-306.
[45] Y. Shi, J. Bao, Z. Yan, and S. Jiang, "Intrusion detection for transportation information security systems based on genetic algorithm-chaos and RBF neural network," in *Proc. 3rd Pacific-Asia Conference on Circuits, Communications and Syste.*, Wuhan, China, 2011.
[46] V. Viduto, C. Maple, W. Huang, and A. Bochenkov, "A multi-objective genetic algorithm for minimising network security risk and cost," in *Proc. International Conference on High Performance Computing and Simulation*, 2012, pp. 462-467.
[47] A. Tamjidyamcholo, "Information security risk reduction based on genetic algorithm," in *Proc. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Kuala Lumpur, Malaysia, 2012, pp. 122-127.
[48] L. Wang, B. Wang, and Y. Peng, "Research the information security risk assessment technique based on Bayesian network," in *Proc. 3rd International Conference on Advanced Computer Theory and Engineering*, 2010, pp. V3-600-V3-604.
[49] N. Feng and X. Yu, "A data-driven assessment model for information systems security risk management," *Journal of Computers (Finland)*, vol. 7, no. 12, pp. 3103-3109, 2012.
[50] R. Sarala, M. Kayalvizhi, and G. Zayaraz, "Information security risk assessment under uncertainty using dynamic Bayesian networks," *International Journal of Research in Engineering and Technology*, pp. 304–309, 2014.
[51] Z. J. A. Lee and L. Y. B. Chang, "Apply fuzzy decision tree to information security risk assessment," *International Journal of Fuzzy Systems*, pp. 265-269, 2014
[52] Y. Fu, Y. L. Qin, and X. P. Wu, "A method of information security risk assessment using fuzzy number operations," in *Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, China, 2008, pp. 1-4.
[53] A. Shameli-Sendi, M. Shajari, M. Hassanabadi, M. Jabbarifar, and M. Dagenais, "Fuzzy multi-criteria decision-making for information security risk assessment," *Open Cybernetics and Systemics Journal*, vol. 6, no. 1, pp. 26-37, 2012.
[54] S. Wu, S. Y. Wang, T. Zhang, and J. M. Zhao, "Multi-level fuzzy-gray comprehensive evaluation of information security risk," in *Proc. International Conference on Management and Service* Science, *MASS*, Wuhan, China, 2010.
[55] X. Wu, Y. Fu, and J. Wang, "Information systems security risk assessment on improved fuzzy AHP," in *Proc. Second ISECS International Colloquium on Computing, Communication, Control, and Management*, Sanya, China, 2009, pp. 365-369.
[56] L. Zhou and Y. Zhou, "Gray relational analysis based method for information security risk assessment," in *Proc. 7th International Conference on Computer Science and Education*, Melbourne, VIC, Australia, 2012, pp. 1086-1089.
[57] M. S. Liu, S. J. Sun, and X. H. Yin, "Research on the evaluation of security risk for e-government information system," in *Proc. the 7th International Conference on Machine Learning and Cybernetics*, 2008, pp. 1404-1409.
[58] T. Zou, J. Han, and L. Zhang, "Research on the fuzzy comprehensive evaluation for information system security risk," in *Proc. International Conference on Electrical and Control Engineering*, 2011, pp. 334-337.
[59] R. Muratkhan and D. Z. Satybaldina, "Quantitative method of information security risk assessment by multicomponent threats," *Life Science Journal*, pp. 372-375, 2014.
[60] S. Fenz, A. M. Toa, and M. Hudec, "Ontology-based generation of bayesian networks," in *Proc. the International Conference on Complex, Intelligent and Software Intensive Systems*, Fukuoka, Japan, 2009, pp. 712-717.

[61] Y. A. Yao, X. B. Ma, H. A. Liu, J. A. Yi, X. A. Zhao, and L.A. Liu, "A semantic knowledge base construction method for information security," in *Proc. 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, 2015, pp. 803-808.
[62] M. M. Stambul and R. Razali, "An assessment model of information security implementation levels," in *Proc. International Conference on Electrical Engineering and Informatics*, Bandung, Indonesia, 2011.
[63] J. Mayer and L. Fagundes, "A model to assess the maturity level of the risk management process in information security," in *Proc. IFIP/IEEE International Symposium on Integrated Network Management-Workshops*, New York, NY, United States, 2009, pp. 61-70.
[64] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," in *Proc. IEEE International Conference on Technologies for Homeland Security, HST*, Waltham, MA, United States, 2012, pp. 457-462.
[65] W. Boehmer, "Dynamic systems approach to analyzing event risks and behavioral risks with game theory," in *Proc. IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing*, pp. 1231-1238, 2011.
[66] K. Beckers, H. Schmidt, J. Kuster, and S. Fassbender, "Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing," in *Proc. Sixth International Conference on Availability, Reliability and Security*, Vienna, 2011, pp. 327-333.
[67] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *Proc. 10th IEEE International Conference on Computer and Information Technology, CIT, 7th IEEE International Conference on Embedded Software and Systems*, Bradford, United Kingdom, 2010, pp. 1328-1334.
[68] A. B. Mxoli, M. A. Gerber, and N. A. Mostert-Phipps, "Information security risk measures for cloud-based personal health records," in *Proc. International Conference on Information Society*, South Africa, 2015, pp. 187-193.

Manuel Alcántara is Peruvian. He studied Mathematics at the Universidad Nacional de Trujillo (UNT), Systems Engineering at Universidad Peruana Union (UPeU). He did a Masters in Computer Science at the Pontificia Universidad Católica del Perú (PUCP) and Ph.D. in Systems Engineering at the Universidad Nacional Federico Villarreal (UNFV). He has a Diploma in International Business Administration from the Universidad Norbert Wiener (UNW) and Diploma in Investigation from the Universidad San Ignacio of Loyola (USIL). He has taught at PUCP, at the University of Lima (UL), UNT, at UNFV, UNW, at UPeU, at Universidad Nacional del Callao (UNAC), at Universidad Nacional Tecnológica de Lima Sur (UNTELS) and at the USIL. He has held various management positions as head of the Office of Information Technology and Communications (UNTELS), Academic Director of CELA (Latin American Administration Center), Director of the School of Systems Engineering in the UNAC. He is a member of the College of Engineers of Peru (CIP 149488), is a member of the College of Mathematics of Peru, member of the Mathematical Association of Peru, Member of the Peruvian Mathematical Society, member of the Peruvian Association of Computer and Information.

Andrés Melgar received the Ph.D. degree in knowledge engineering from Federal University of Santa Catarina (UFSC), Florianopolis, Brazil, the Master degrees in Biomedical Engineering and the Bachelor of Science and Engineering from Pontificia Universidad Católica del Perú (PUCP), Lima, Peru. He runs the Pattern Recognition and Applied Artificial Intelligence Group (GRPIAA) at PUCP. He works at PUCP as an associate professor at Engineering Department. He has served as program coordinator of the informatic engineering program. He is a former research director of informatic engineering section at PUCP. He is currently researching issues related to the semantic Web, information retrieval, information extraction and machine learning.