A SYSTEMATIC REVIEW OF INFORMATION SECURITY RISK ASSESSMENT

L. PAN & A. TOMLINSON
Information Security Group, Royal Holloway University of London.

ABSTRACT

Many standards exist to guide the process of risk assessment, particularly in the field of information security. This leads to many, subtly different, definitions of risk analysis, evaluation and assessment. Consequently, researchers often confuse these terms and disciplines, which leads to further confusion within the community. In this sense, it is important to come to a common understanding of the processes and terminology to clarify research in this area. A common approach to achieve this goal is to carry out a literature review. This paper takes a formal approach to the literature review based on the ideas of the Cochrane group. The result is a systematic review of risk assessment in the field of information security. We present a systematic review of over 80 research papers published between 2004 and 2014. The main contribution of our paper is to construct a classification of these published papers into seven types. This classification aims to help researchers obtain a clear and unbiased picture of the terminology, developments and trends of information security risk assessment in the academic sector.

Keywords: information security, ISO 27005, risk analysis, risk assessment, systematic review.

1 INTRODUCTION

Different standards take different approaches to the processes of Information Security Risk Assessment (ISRA). For instance, SP800-30 [1], ISO 27001 [2] and ISO 27005 [3] provide the slightly different definitions and procedures for ISRA. Of these three standards, ISO 27005 provides more accurate definitions for each stage of the ISRA process. Most literatures describe abundant different taxonomies, frameworks and methods for ISRA [4]. Shameli-Sendi *et al.* [5] provide a taxonomy of ISRA which focuses on risk analysis. In this taxonomy, the risk analysis approach called appraisement is divided into qualitative, quantitative, and hybrid. Shamala *et al.* [6] present a conceptual framework of comparisons among well-documented ISRA guidelines including NIST 800-30, OCTAVE and ISRAM. Other authors are interested in the improvement of current risk analysis approaches by applying fuzzy theory [7, 8] and AHP (Analytic Hierarchy Process) theory [9, 10].

However, to our knowledge, there has been no systematic overview of the ISRA research to analyse the emphasis of the work and the direction of future research. Consequently, this paper will apply the methodology of systematic review not only to summarize the related research papers, but also to present a classified framework of these papers. In order to not to confuse the phrases of risk analysis, risk assessment and risk evaluation, we will use their definitions from ISO 27005 in our systematic review. The aim of the classification framework is to help researchers obtain a clear picture about the research areas. According to this classification, researchers can find some study entry points in this sector. Researchers may also learn the advanced ISRA methods and find the connections between organizational level and academic level from this systematic review.

This paper is part of the Proceedings of the 10th International Conference on Risk Analysis (RISK 2016)
www.witconferences.com

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V6-N2-270-281

The rest of this paper is structured as follows: Section 2 introduces the research methodology of systematic review; section 3 presents the general statistical results and a classification framework of reviewed ISRA papers; and section 4 discusses all parts of this classification framework. Section 5 states the conclusions and the future research directions of ISRA.

2 SYSTEMATIC REVIEW (SR)

Medicine and health were the initial subjects of applying a systematic research review. The Cochrane Collaboration group developed the systematic review process into the professional methods called the Cochrane Review [11]. A Cochrane Review is a systematic review in healthcare and reflects the findings of updated studies[1]. However, this approach is also used in other subjects for collecting published literature data and assessing the current development trends [12]. Some research questions may be answered by a systematic review of as many relevant research papers as possible. The traditional literature review can be an ad-hoc process which may be incomplete or unbalanced [13]. Systematic reviews can overcome this problem and provide accountable and replicable results. This approach adopts explicit and transparent methodologies and a standard process to synthesize all existing research work and provide an unbiased result [13].

This paper for the first time proposes an idea of employing a systematic review to analyse and synthesise papers over a 10 year period in the field of ISRA. The process is carried out as follows: first, define explicit research questions; second, conduct the literature search; third, select the relevant literature according to the paper's title, abstract and keywords; fourth, extract and synthesize data of relevant papers; finally, classify the data and explain the classification results.

2.1 Research methodology of SR

This section introduces the steps of the systematic review including research questions, review protocol, selection criteria, data extraction and synthesis.

2.1.1 Research questions

In order to know the scope and emphasis of ISRA study, this section sets the following research questions:

1. What kinds of ISRA methods are mainly studied by researchers?
2. What are the current research categories?
3. Which subjects are likely to become the future research focus of ISRA?

2.1.2 Review protocol

We defined a set of searching scope and keywords for the review. The literature is selected from Google Scholar, ACM Digital Library, Science Direct, Web of Science, Wiley InterScience, DBLP, IEEE Digital Library, Springer Link, Elsevier by using a set of keywords such as information security risk assessment, security risk assessment, assessing risk of information security. Moreover, we restricted our search to publications from 2004 to 2014.

2.1.3 Selection criteria

After searching the literature, we now define the selection criteria to answer the research questions above. The selection criteria are as follows:

- The paper is written in English
- The paper is peer reviewed
- The title contains a similar meaning of risk assessment and at least one word of information security
- The paper can be downloaded free of charge
- The title clearly mentions a research, e.g. healthcare, cloud
- The paper specifies the method of risk analysis/risk identification/risk evaluation

2.1.4 Data extraction and synthesis

107 research papers were found in the original search. According to the above criteria, we filtered these papers and 80 publications were selected as the final set of relevant papers.

3 SR OF ISRA RESULTS

This section introduces the general statistical results of our search and presents a classification framework of this literature. The results show the annual distribution of published papers and the types of application areas.

3.1 General statistical descriptions

Of the 80 publications, 38 were from journals, 37 from conferences and 5 from symposia. These papers were published in 78 different types of journals, conferences and symposiums such as "Transactions on Dependable and Secure Computing (TDSC)". This illustrates the data sample is more convincing due to the diversity of paper collections.

In addition, the types of industries are diverse. For instance, E-government [14], supply chain management [15], E-health [16], E-science [17], student performance [18], chlorine processing system [19], transportation industry [20], power systems [21], cloud computing [22–25], mobile applications [26] and so on. The development of ISRA in these industries illustrates that ISRA is becoming increasingly important not only traditional industries, but also other emerging domains such as mobile and cloud computing.

3.2 Classification framework of ISRA

Definitions of risk analysis, risk assessment and risk evaluation vary for each of the selected papers. This can be confusing. In order to distinguish these terms explicitly, it is necessary to

Table 1: Classification framework of research types in ISRA.

Research categories	Number of Studies
Risk identification	5
Comparison of risk analysis	4
Improvement of risk analysis	32
Comparison of frameworks	2
Improvement of frameworks	29
Case study	4
Others	4

unify the definitions about them. Thus, this paper applies the clear and understandable ISRA definitions of ISO 27005. Table 1 shows the categories and the number of relevant papers.

4 DISCUSSIONS OF RESULTS OF THE SYSTEMATIC REVIEW

We have classified the selected papers into seven types. The detailed contents of these categories will be discussed in this section. We discuss the features of each type and the current study emphases of these types.

4.1 Risk identification

"Risk identification is the process of finding, recognizing and describing risks [3]." One of the earlier risk identification methods is Hierarchical Holographic Modelling (HHM), which was first proposed by Yacov Y. Haimes in 1981 [27], and then was applied at risk identification in 1995 [28]. HHM presents a detailed framework to identify risks from eight main parts of the system [28]. However, HHM is not often mentioned by current researchers. In fact, HHM is more difficult to identify the enterprise and operation risks [29]. Brainstorming and questionnaires are the general methods of risk identification applied most frequently by most organizations. However, these general methods are too objective and time-consuming for users [30].

In order to improve the efficiency and accuracy of risk identification, Shed-den et al. [31] propose a business practice perspective, which includes a more complete list of information assets and helps organizations to identify risks efficiently. Moreover, for the sake of the non-specialist users who have lack of knowledge of information security, Ya-chi Chu et al. classify assets into five types: hardware, software, information, people and services and present very detailed content for each type [30]. In addition, knowledge-based methods [32] are also an effective means of risk identification. Finally, Padyab et al. present a genre-based method for identifying risk named GBM-OA (Genre based method-OCTAVE Allegro) [33].

The papers reviewed indicate that Shedden [31, 34] is one of the key authors in the field of risk identification. Her papers are cited frequently by other authors. Shedden also illustrates that the technical infrastructure is the core concern in current risk identification standpoint [31]. Most of methods of risk identification above are proposed from academic level, although Shedden et al. make some connection from an organizational perspective. Furthermore, existing methods of risk identification cannot deal with important factors such as asset leakage, user-created assets and critical knowledge [31]. Likewise, most publications prefer to focus on identifying the risks more efficiently and accurately rather than valuing these risks. We argue that the approaches to risk identification should be not only finding the risks, but also valuing them. Future research on this topic focuses on applying the current academic methods of risk identification to the real world.

4.2 Risk analysis

"Risk analysis is the process to comprehend the nature of risk and to determine the level of risk" [3] In the systematic review, there are 32 papers on the improvement of risk analysis methods and 4 papers about the comparison of them. The results of risk analysis are the basis of decision-making for risk evaluation [3]. Risk analysis depicts the magnitude of a risk and expresses this in terms of a combination of consequences and likelihood [3]. In general, the methods of risk analysis can be divided into three types: qualitative, quantitative and synthetic analysis [25].

"factor analysis, logical analysis, historical comparative and Delphi method" [35] are the typical qualitative methods; "cluster analysis, time series model, regression model and decision tree method" [35] are the typical quantitative methods; the typical synthetic methods contain "hierarchical analysis, probabilistic risk assessment and fuzzy comprehensive evaluation methods" [35].

These methods to some extent are not without drawbacks due to their respective nature. Qualitative methods are subjective and rely on the knowledge and experience of the evaluators, while Quantitative methods depend on the quality of data [35, 36]. The synthetic methods diminish the subjectivity of qualitative methodology and improve the accuracy of quantitative methods by adding the expert's knowledge. Consequently the mainstream of research in risk analysis methods is developing synthetic methods. As we know, impact and likelihood are two important metrics for risk analysis. Hence, developing risk analysis methods is mainly focused on how to obtain more accurate and effective values of impact and likelihood.

4.2.1 Risk analysis-comparison

Research comparing risk analysis tools in our systematic review considered the advantages and disadvantages of quantitative or qualitative risk analysis methods. For instance, Mingchang Lee compared these two types of methods from the view of economics [37]. He suggests that quantitative methods can be used for cost-benefit analysis and to obtain more accurate results, but that they rely on the scale of measurement body [37]. Qualitative methods, however, make it more difficult to provide a cost-benefit analysis.

Chien-Cheng Huang compares the five common methods of risk scenario analysis and points out the features and problems of every method [19].

In addition, there are many ways to classify the risk analysis methods such as knowledge-based and model-based [35], software-based and paper-based methods [38], asset-based [39, 40] and business process-based [41]. For instance, ISRAM (Information Security Risk Analysis Method) [38] is a quantitative and paper-based method. It measures the complex information systems by two separate and independent surveys and analyses the data from these surveys. Though ISRAM is easy to use, without sophisticated mathematical tools, it depends on the quality of the survey results and the knowledge of participants.

4.2.2 Risk analysis-improvement

In the 32 papers presenting improvements, 12 papers mention AHP (Analytic Hierarchy Process) and fuzzy theory. The authors of these papers combine AHP or fuzzy theory or both, with another typical qualitative or quantitative risk analysis method to reduce the subjectivity of qualitative approach. However, most of these improved quantitative methods will adopt the expert's opinion or the result of a survey as the input data. For instance, Karaba-cak and Sogukpinar apply the real-life statistical data of a survey as input data to analyse risks properly [38]. Moreover, three papers [20, 36, 42] adopt the expert's assessment as the input data and then use the AHP or fuzzy theory to reduce the subjectivity of these input data.

The reason that AHP and fuzzy theory chosen in the research of risk analysis methods is because these techniques can overcome the flaws in the nature of qualitative and quantitative tools. Thomas L. Saaty presented the concept of AHP in the 1970s and applied it to study complicated problems [21]. AHP decomposes the complex problems into several sub questions and analyses these sub questions independently [21]. AHP can provide more accurate data if it is used with quantitative methods. But many authors apply fuzzy theory to reduce the subjectivity of qualitative risk analysis [36].

Chang and Lee [42] apply fuzzy expert systems to reduce the subjectivity of likelihood to get more objective results. Moreover, risk scenario analysis methods are frequently used for the improvement of synthesis methodologies except AHP and fuzzy theory. Whether risk scenarios or AHP or fuzzy theory, soft computing and hybrid models look likely to become the future research direction of risk analysis methods [37].

Expert opinion is the current main type of input data used in the risk analysis for information security. However, another type of input data is historical data, although few authors have investigated this area. Imamverdiyev [43] analyses risks by using input data from the database of AzScienceNet. In this paper, the distribution of the maximum number of incidents is described as a Weibull distribution. Nevertheless, this paper discusses only the probability distribution of the incident, and does not provide further knowledge about the loss distribution.

In the improvement process of risk analysis approaches, some authors mention the dependencies among threats, vulnerability and assets and security controls. Jaya Bhattacharjee et al. propose the idea that it is important to include the dependencies among information security risks in a risk analysis method [40]. Further interdependencies that should be considered are the interrelations among security controls [36].

To sum up, the current research directions of risk analysis approaches can be divided into two parts: comparison and improvement as illustrated in Fig. 1. The comparison is about the benefits and drawbacks of the current qualitative and quantitative methods. As far as improvement is concerned, most papers improve the current approaches by combining fuzzy theory and AHP to construct a hybrid model. These hybrid models can obtain more accurate data for quantitative tools and reduce the subjectivity of qualitative methods [36]. All in all, most risk analysis approaches use the expert opinion as input data, and then assesses the risks by the hybrid model of AHP or fuzzy theory.

4.3 Framework-comparison

In our systematic review, we found that two papers compare ISRA methods from conceptual structures. Shamala et al. [6] select well-documented methods and compare them by using a conceptual framework. This comparison can assist organizations to choose the most suitable ISRA method by providing a general overview of the ISRA process and ISRA requirements in this conceptual framework. Unfortunately, the authors did not consider the widely-used ISO 27005 standard in their comparison. Moreover, they did not offer any advice as to which methodologies can be applied at which types of organizations. Korman et al. [44] also apply

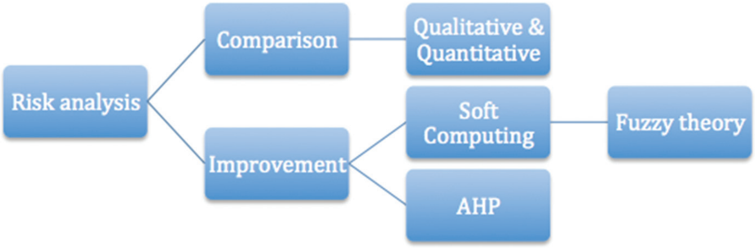

Figure 1: Current research directions of risk analysis.

the conceptual framework to compare and analyse the ISRA methods. In his analysis, more well-documented ISRA methods are selected as input, including ISO 27005. In addition, the study shows the differences of these methods on the extent of input information or data collected by statistical tools. By contrast, Shamala et al. do not consider the extent of input data for users.

4.4 Framework-improvement

In the category of frameworks, most authors try to improve the whole process of ISRA by following different standards like ISO 27005 and NIST SP800-30. They propose risk identification methods from the standpoint of defined subjects in the improvement. For instance, Sameer Hasan Albakri et al. [24] suggest that it is more realistic and easier to identify risks from two views of cloud clients and cloud service providers on the subject of cloud computing. Yiming Jing et al. [26] identify the risks from users' coarse expectations in mobile applications.

The improvement of risk identification methods in the category of frameworks is just giving a more show list to identify risks or assets from different users' views. However, this does not give a new perspective. For the methods of risk analysis in the framework, the authors make the calculations of risk level more objectively and efficiently. However, more subjects or industries are using the framework of ISRA, especially in the field of healthcare and cloud computing. But academic researches are not advanced enough for the demand of these two areas. Researchers could focus on these areas and propose more practical methods or models to improve the process of ISRA.

Overall, the authors seek to enrich the framework to a defined subject area comparing with the process of ISRA of ISO 27005. They give more detailed steps for identifying risks from different views and calculating the value of the risk by specific risk analysis methods and setting the criteria for accepting the risks.

4.5 Case study

Four papers consider ISRA from the solely view of a case studies. These papers indicate that ISRA had been applied in healthcare and student performance. Coleman [45] describes a good example on the applications of OCTAVE in different scale healthcare organizations. In fact, OCTAVE provides more freedom and considers the unique needs of organizations in the process of ISRA. However, Workshop, which is used to collect data in OCTAVE, has some limitations because the process of identifying risks by conducting the workshops may increase the relative overhead and is too time-consuming for large scale organizations [46]. Additionally, Caralli et al. [46] do not provide the detailed calculation method of risk score, so we have no idea whether the method is suitable or objective. Yeo et al. [47] discuss the factors which will affect the practical ISRA process and examine the effects of these factors by a large university.

From the case studies, we know the authors apply ISRA in education and healthcare subjectively at the early development stage of ISRA. However, in academia, the authors refer less to other types of organizations and mention some detailed examples of a practical ISRA. Of course we cannot say that ISRA is applied less in other types of organizations, but fewer authors focus on studying the real case in real organizations. These case studies are not so powerfully reliable in their conclusions due to only investigating one case.

4.6 Others

The "Others" category concludes our classification of ISRA research. Work in this category includes the application of cost analysis to ISRA and the future direction of ISRA development. The classification of others provides some special and rare research directions for studying ISRA. It is interesting to discuss the impact of other roles, not only facilitators, of ISRA in different systems. Furthermore, it is also worthy to consider the analysis of ISRA from the economic view like cost-benefit analysis and game theory.

4.7 Risk evaluation

"Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable" [3]. Some papers mention risk evaluation, but they do not present a detailed discussion on the selection of risk criteria. Therefore, there is scope for research in risk evaluation, focusing on choosing risk criteria and making the compared results more fair, suitable, efficient and accurate. However, risk evaluation does not appear to be a popular research topic, even with mentioned, it is treated as risk analysis. We suggest that risk evaluation, and the risk criteria selection, may be a new research area and it is possible for this to become a new and valued research area in the field of ISRA.

5 CONCLUSION

Systematic reviews examine the existing research papers in ISRA and present an unbiased view of current research activities. In this paper, the systematic literature review provides a classification framework to position current study directions between 2004 and 2014. This framework divides the research papers into seven parts as follows. Firstly, risk identification is the first and most important step in the whole assessment progress. However, the existing methods of risk identification cannot deal with some important factors such as asset leakage, user-created assets and critical knowledge [31]. Secondly, the class of risk analysis contains two sub parts: comparison and improvement. The comparison mainly focuses on the benefits and drawbacks of quantitative and qualitative risk analysis approaches. Another sub part of the improvement is about how to obtain more objective and accurate risk scores by improving the calculation of the likelihood or impact. The systematic review suggests that fuzzy theory is widely used to reduce the subjectivity on the calculations of risk scores.

In the class of ISRA frameworks, researchers enrich the assessment framework for a defined subject area. They provide more detailed steps for identifying risks from different views; suggest how to calculate the value of the risk by specific risk analysis methods; and set the criteria for accepting the risks. The related papers of case studies show how ISRA is applied in education and healthcare disciplines in the early development stage. The class of others provides some special and rare research directions for studying ISRA. This category consider the impact of different roles such as facilitators, in different information systems. Furthermore, it may also be desirable to investigate ISRA from the economic view such as cost-benefit analysis and game theory.

However, ISO 27005 and the reviewed papers rarely mention the methods of collecting and managing the information (or data); which suggests that these may be difficult problems. And the lack of training data or "real-world" data evident in our review is becoming an urgent research problem in ISRA [48, 49]. For current approaches to risk analysis, most propose to deal with general threats rather than focus on specific types of information security risks. While this may be desirable from an academic perspective, from a practical perspective it leaves a lot of work to be done. In addition, it is difficult to automatically assess information security risks with assessment software systems. Thus, a potential research direction could be to focus on data management in a practical process of ISRA. In other words, it is important to know the input data in a risk assessment, and the kinds of methods that can be used to collect and analyse the data of risks efficiently, effectively and accurately.

REFERENCES

[1] NIST, SP 800-30, Guide for Conducting Risk Assessments, 2012.

[2] ISO, 27001:2005, Information technology - security techniques - information security management systems - requirements. *International Organization for Standardization,* 2005.

[3] ISO, 27005:2011, Information technology-security techniques-information security risk management. *International Organization for Standardization,* 2011.

[4] Saleh, M.S. & Alfantookh, A., A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics,* 9(2), pp. 107–118, 2011.
http://dx.doi.org/10.1016/j.aci.2011.05.002

[5] Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M., Taxonomy of information security risk assessment (isra). *Computers & Security,* 57, pp. 14–30, 2016.
http://dx.doi.org/10.1016/j.cose.2015.11.001

[6] Shamala, P., Ahmad, R. & Yusoff, M., A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications,* 18(1), pp. 45–52, 2013.
http://dx.doi.org/10.1016/j.jisa.2013.07.002

[7] Feng, N. & Li, M., An information systems security risk assessment model under uncertain environment. *Applied Soft Computing,* 11(7), pp. 4332–4340, 2011.
http://dx.doi.org/10.1016/j.asoc.2010.06.005

[8] Lee, Z.J. & Chang, L.Y., Apply fuzzy decision tree to information security risk assessment. *International Journal of Fuzzy Systems,* 16(2), pp. 265–269, 2014.

[9] Awad, G.A., Sultan, E.I., Ahmad, N., Ithnan, N. & Beg, A., Multi- objectives model to process security risk assessment based on ahp-pso. *Modern Applied Science,* 5(3), p. 246, 2011.
http://dx.doi.org/10.5539/mas.v5n3p246

[10] Eren-Dogu, Z.F. & Celikoglu, C.C., Information security risk assessment: Bayesian prioritization for ahp group decision making. International Journal of Innovative Computing, Information and Control, 8, pp. 8001–8018, 2012.

[11] Hannes, K., Booth, A., Harris, J. & Noyes, J., Celebrating methodological challenges and changes: reflecting on the emergence and importance of the role of qualitative evidence in cochrane reviews. Systematic Reviews, 2(1), p. 1, 2013.
http://dx.doi.org/10.1186/2046-4053-2-84

[12] Ader, H.J. & Mellenbergh, G.J., Advising on Research Methods: a Consultant's Companion, Johannes van Kessel Publishing, 2008.

[13] Kitchenham, B.A. & Charters, S., Guidelines for performing systematic literature reviews in software engineering, *EBSE Technical Report*, 2007.

[14] Wei, G., Xhang, X., Zhang, X. & Huang, Z., Research on e-government information security risk assessment-based on fuzzy ahp and artificial neural network model.

Networking and Distributed Computing (IC-NDC), First International Conference on, IEEE, pp. 218–221, 2010.
http://dx.doi.org/10.1109/icndc.2010.52

[15] Roy, A., Gupta, A. & Deshmukh, S., Information security risk assessment in SCM. Industrial Engineering and Engineering Management (IEEM), 2013 IEEE International Conference on, IEEE, pp. 1002–1006, 2013.
http://dx.doi.org/10.1109/ieem.2013.6962561

[16] Wei, J., Lin, B. & Loho-Noya, M., Development of an e-healthcare information security risk assessment method. Journal ofDatabase Management (JDM), 24(1), pp. 36–57, 2013.

[17] Mouw, E., van't Noordende, G., Louter, B. & Olabarriaga, S.D., A model-based information security risk assessment method for science gateways. IWSG, 2013.

[18] Dark, M.J., Assessing student performance outcomes in an information security risk assessment, service learning course. Proceedings ofthe 5th Conference on Information Technology Education, ACM, pp. 73–78, 2004.
http://dx.doi.org/10.1145/1029533.1029552

[19] Huang, C.C., Farn, K.J. & Lin, F.Y.S., A study on implementations of information security risk assessment: Application to chlorine processing system of water treatment. IJ Network Security, 16(4), pp. 377–384, 2014.

[20] Xiangmo, Z., Ming, D., Shuai, R., Luyao, L. & Zongtao, D., Risk assessment model of information security for transportation industry system based on risk matrix. Applied Mathematics & Information Sciences, 8(3), pp. 1301–1306, 2014.
http://dx.doi.org/10.12785/amis/080345

[21] Ye, Y., Lin, W.M., Deng, S. & Zhang, T., A practical solution to the information security risk evaluation problems in power systems. *2014 International Conference on Future Computer and Communication Engineering (ICFCCE 2014),* Atlantis Press, 2014.
http://dx.doi.org/10.2991/icfcce-14.2014.9

[22] Latif, R., Abbas, H., Assar, S. & Ali, Q., Cloud computing risk assessment: A systematic literature review. Future Information Technology, Springer, pp. 285–295, 2014.

[23] Makarevich, O., Mashkina, I. & Sentsova, A., The method of the information security risk assessment in cloud computing systems. *Proceedings of the 6th International Conference on Security of Information and Networks,* ACM, pp. 446–447, 2013.
http://dx.doi.org/10.1145/2523514.2527021

[24] Albakri, S.H., Shanmugam, B., Samy, G.N., Idris, N.B. & Ahmed, A., Security risk assessment framework for cloud computing environments. *Security and Communication Networks,* 2014.

[25] Peiyu, L. & Dong, L., The new risk assessment model for information system in cloud computing environment. *Procedia Engineering,* 15, pp. 3200–3204, 2011.
http://dx.doi.org/10.1016/j.proeng.2011.08.601

[26] Jing, Y., Ahn, G., Zhao, Z. & Hu, H., Towards automated risk assessment and mitigation of mobile application.

[27] Haimes, Y.Y., Hierarchical holographic modeling. *Systems, Man and Cybernetics, IEEE Transactions on,* 11(9), pp. 606–617, 1981.

[28] Haimes, Y.Y., Lambert, J., Li, D., Schooff, R. & Tulsiani, V., Hierarchical holographic modeling for risk identification in complex systems. Systems, Man and Cybernetics, 1995. Intelligent Systems for the 21st Century., IEEE International Conference on, IEEE, volume 2, pp. 1027–1032, 1995.
http://dx.doi.org/10.1109/icsmc.1995.537904

[29] Ting, J.S.L., Tsang, A.H.C. & Kwok, S.K., Hybrid risk management methodology: a case study. *International Journal of Engineering Business Management,* 1(1), pp. 25–32, 2009.

[30] Chu, Y.C., Wei, Y.C. & Chang, W.H., A risk recommendation approach for information security risk assessment. Network Operations and Management Symposium (APNOMS), 2013 15th Asia-Pacific, IEEE, pp. 1–3, 2013.

[31] Shedden, P., Smith, W. & Ahmad, A., Information security risk assessment: towards a business practice perspective, *Proceedings of the 8th Australian Information Security Management Conference*, Edith Cowan University, Perth Western, Australia, 2010.

[32] Guan, J.Z., Lei, M.T., Zhu, X.L. & Liu, J.Y., Knowledge-based information security risk assessment method. *The Journal of China Universities of Posts and Telecommunications,* 20, pp. 60–63, 2013.
http://dx.doi.org/10.1016/S1005-8885(13)60220-4

[33] Padyab, A.M., Paivarinta, T. & Harnesk, D., Genre-based assessment of information and knowledge security risks. *System Sciences (HICSS), 2014 47th Hawaii International Conference on,* IEEE, pp. 3442–3451, 2014.
http://dx.doi.org/10.1109/hicss.2014.428

[34] Shedden, P., Scheepers, R., Smith, W. & Ahmad, A., Incorporating a knowledge perspective into security risk assessments. *Vine,* 41(2), pp. 152–166, 2011.
http://dx.doi.org/10.1108/03055721111134790

[35] Fu, S. & Xiao, Y., Strengthening the research for information security risk assessment. *International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering,* **9**, pp. 386–392, 2012.

[36] Lo, C.C. & Chen, W.J., A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications,* 39(1), pp. 247–257, 2012.
http://dx.doi.org/10.1016/j.eswa.2011.07.015

[37] Lee, M.C., Information security risk analysis methods and research trends: Ahp and fuzzy comprehensive method. International Journal ofComputer Science, 2014.

[38] Karabacak, B. & Sogukpinar, I., Isram: information security risk analysis method. Computers & Security, 24(2), pp. 147–159, 2005.
http://dx.doi.org/10.1016/j.cose.2004.07.004

[39] Zhiwei, Y. & Zhongyuan, J., A survey on the evolution of risk evaluation for information systems security. Energy Procedia, 17, pp. 1288–1294, 2012.
http://dx.doi.org/10.1016/j.egypro.2012.02.240

[40] Bhattacharjee, J., Sengupta, A. & Mazumdar, C., A formal methodology for enterprise information security risk assessment. Risks and Security of Internet and Systems (CRiSIS) International Conference on, IEEE, pp. 1–9, 2013.
http://dx.doi.org/10.1109/crisis.2013.6766354

[41] Khanmohammadi, K. & Houmb, S.H., Business process-based information security risk assessment. *Network and System Security (NSS) 4th International Conference on,* IEEE, pp. 199–206, 2010.
http://dx.doi.org/10.1109/nss.2010.37

[42] Chang, L.Y. & Lee, Z.J., Applying fuzzy expert system to information security risk assessment -a case study on an attendance system. Fuzzy Theory and Its Applications (iFUZZY) International Conference on, IEEE, pp. 346–351, 2013.

[43] Imamverdiyev, Y., An application of extreme value theory to e-government information security risk assessment. AICT, International Conference on Application of Information and Communication Technologies, IEEE, pp. 1–4, 2013.
http://dx.doi.org/10.1109/icaict.2013.6722700

[44] Korman, M., Sommestad, T., Hallberg, J., Bengtsson, J. & Ekstedt, M., Overview of enterprise information needs in information security risk assessment. Enterprise Distributed Object Computing Conference *(EDOC), IEEE* 18th *Internationa*l, IEEE, pp. 42–51, 2014.
http://dx.doi.org/10.1109/edoc.2014.16

[45] Coleman, J., Assessing information security risk in healthcare organizations of different scale. International Congress Series, Elsevier, **1268**, pp. 125–130, 2004.

[46] Caralli, R.A., Stevens, J.F., Young, L.R. & Wilson, W.R., Introducing octave allegro: Improving the information security risk assessment process. *Technical Report*, DTIC Document, 2007.

[47] Yeo, A.C., Rahim, M.M. & Miri, L., Understanding factors affecting success of information security risk assessment: The case of an Australian higher educational institution. PACIS Proceedings, p. 74, 2007.

[48] Baker, W.H., Rees, L.P. & Tippett, P.S., Necessary measures: metric-driven information security risk assessment and decision making. Communications of the ACM, 50(10), pp. 101–106, 2007.
http://dx.doi.org/10.1145/1290958.1290969

[49] Gao, G.H., Li, X.Y., Zhang, B.J. & Xiao, W.X., Information security risk assessment based on information measure and fuzzy clustering. Journal of Software, 6(11), pp. 2159–2166, 2011.
http://dx.doi.org/10.4304/jsw.6.11.2159-2166