Available online at http://jcst.rsu.ac.th
Formerly Rangsit Journal of Arts and Sciences (RJAS)

Journal of Current Science and Technology, January-June 2018 JCST Vol. 8 No. 1, pp. 33-40
Copyright ©2011, Rangsit University ISSN 2630-0583 (Print)/ISSN 2630-0656 (Online)

Fuzzy rule-based risk management under ISO/IEC27001:2013 standard for information security

Pichit Boonkrong* and Chuleekorn Nuansomsri

College of Digital Innovation and Information Technology (DIIT), Rangsit University, Patumthani 12000, Thailand

*Corresponding author; E-mail: pichit.bk@rsu.ac.th

Submitted 20 September 2017; accepted in final form 26 June 2018
Available online 29 June 2018

Abstract

This paper aims to identify, assess and offer management guideline of operational risk on information and communication technology (ICT) under ISO/IEC 27001:2013 standard using Mamdani fuzzy model-based management. Qualitative research methodology and research standard questionnaires were employed for collecting data from 21 surveyees related to ICT fields in January 2017. The fuzzy logic-based risk matrices were used in risk assessment. The uncertainties and imprecision of the complex risk management are better described by fuzzy rule-based reasoning. From the case study, the results show that the risk on ICT has high levels in five criteria including security policy for information, information security related to personnel, physical and environmental security, management in information security and organizational continuity management. Guidelines on risk management are also introduced as an integral part of good management.

Keywords: *fuzzy set, IEC, information security, ISO, Mamdani fuzzy model, risk management*

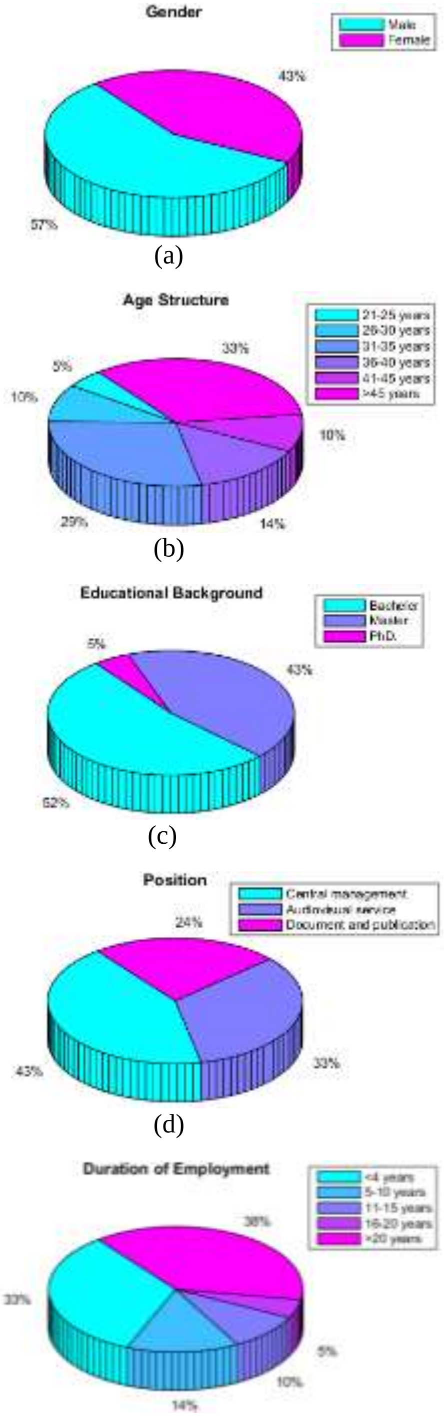
1. Introduction

Recently, information and communication technology (ICT) has played a vital role in human life. It empowers human to catch sight of information and makes the business units more competitively intense. To respond and provide fast customer service, making effective business decisions requires the accuracy of quality information (Mansell, 1999; Ruddock, 2006). Thus, the information system becomes the core asset of the organization, which must be prioritized and budgeted to develop, update and maintain consistently. When information systems become more important to the organization, maintaining security and safety should be respectively increased. If the information system is deteriorated, the organization will also be impacted by operations that damage the organization (Shenkir & Walker, 2006; Pinder, 2006; Ciborra, 2006).

Risks on ICT can arise from various threats such as cyber-terrorism, computer viruses, spyware, or even natural disasters (Segars & Grover, 1996; Straub & Welke, 1998; Teneyuca, 2001). As a consequence, organizations start to realize and recognize the importance of implementing measures to protect information security. Previously, the most commonly and internationally standard used in organizational information security strategy was ISO/IEC 27001:2005 highlighting on the internal control through policies, procedures and risk assessment (Capuder, 2004; Groves, 2003; Saint-Germain, 2005; Solms, 2001). The context in ISO/IEC 27001:2005 is to emphasis technological processes rather than business processes and it was used as the low level guideline for ICT security describing the more guidance on how control objectives must be precisely operated. To ensure business continuity, mitigate business risk, maximize return on investment and business opportunities, ISO/IEC 27001:2005 defined ICT security as a vital factor that an organization must perform. Under ISO/IEC 27001:2005 standard, 133 controls and 11 aspects including risk assessment, security policy, organizational security structure, human resources security, physical and environmental security, communications and operations management, accessibility control, information security incident management, corporate continuity management and compliance were considerably counted (Humphreys, 2005; Humphreys, 2011). Later on, ISO/IEC 27001:2005 had been revised as the new international standard for information security management systems, known as ISO/IEC 27001:2013. The revision of new information security management has 114 controls and 14 criteria including human resource security, information security policy, physical and environmental security, organization of information security, assess control, cryptography, operations security, communication security, system acquisition development and maintenance, information security incident management, supplier relationship, asset management, information security aspects of business continuity management and compliance (Humphreys, 2016).

Risk is the effect of uncertainties. Thus, risk management is one of important strategic tools for effective management and decision-making since it is able to reduce losses that will damage the organization. In risk management, the issues in identifying, assessing, monitoring, making decisions on and communicating risk are taken into account. Technically, risks can be estimated by hazard matrices, risk graphs and risk matrices (Berg, 2010; Hu et al., 2007; Hussey, 1978; Takács, 2011). Risk assessment matrix is the most common template for assessing and monitoring risks. Traditionally, the risk matrix is defined as the product between likelihood and impact (Cox, 2008; Hussey, 1978; Elsayed, 2009; Philip, Bratvold, & Bickel, 2014). As a result, the relative importance between likelihood and impact produces risk index with the risk assessment matrix of $A=[a_{ij}]_{5\times5}$ where $a_{ij}=i\times j$. Here, the subscripts *i* and *j* are the degree of likelihood and impact, respectively. However, it is quite imprecise to assign the degree of likelihood and impact due to various sources of uncertainty and vagueness from internal and external sources. To deal with the mentioned problem, the classical risk matrix was reformulated into fuzzy risk matrix using the conceptual scheme of fuzzy inference (Elsayed, 2009; Karwowski & Mita, 1986; Mamdani & Assilian, 1975; Markowski & Mannan , 2008; Philip et al., 2014; Wu, Cheng, Hu, & Zhou, 2013; Zadeh, 1973). If-then rules are imposed to process the fuzzy value of linguistic variables and the fuzzy risk surface is then obtained. Therefore, it is strongly recommended that fuzzy risk matrix should be introduced as a mandatory annex in risk management on ICT.

This paper aims to identify, assess and offer management guideline of operational risk on ICT under ISO/IEC 27001:2013. The framework of fuzzy risk management is theoretically illustrated in Section 2. From then, numerical results concerning risk assessment are presented in Section 3, followed by conclusion and discussion in Section 4.



(a)

(b)

(c)

(d)

(e)

Figure 1 General information concerning the surveyees

2. Risk management on ICT

It is noted that systematic risk management on ICT is the key factor of organizational operations including data storage, use of computer equipment and network communications. This study considers risk management of ICT under ISO/IEC 27001:2013 standard to explore the risk level and risk management guidelines in organization.

2.1 Experimental design

Based on ISO/IEC 27001:2013 standard, all 14 criteria were brought in to the questionnaires. The questionnaires were delivered to 21 staffs who work in Data Centre and Information Technology Service Centre, Rangsit University in late January, 2017. Demographic information of the 21 surveyees including gender, age, education, positions and duration of employment are presented as pie charts in Figure 1. In the questionnaires, likelihood and impact were classified into 5 levels ranging from very low, low, medium, high and very high. When the questionnaires were returned, the risk indices is calculated through matrix and fuzzy risk matrix as illustrated in Section 2.2. Then, the risk index from each criterion was ranked according to its value and the criteria with high risk indices were intimately focused for establishing the proactive plan on risk management.

2.2 Fuzzy rule-based risk assessment

In practice, the likelihood and impact inputs are usually associated with vague or imprecise judgment which is fuzzy value. Thus, the system needs to be reformulated using conceptual idea in fuzzy inference. The process begins with defining linguistic variables of each crisp input. After that, fuzzy rules are created to describe how fuzzy inference system (FIS) should make a decision based on the input and output variables. In general, there are three main steps in fuzzy inference as following steps:

Step 1 (*Fuzzification*): The crisp input is transformed into fuzzy input through fuzzification, namely input membership function (MF), e.g., $\mu_A(x)$ is the membership in class *A* of input *x*. Popular types of membership functions are triangular, trapezoidal, Gaussian, bell-shaped, S-shaped and Z-shaped membership functions.

Step 2 (*Rule evaluation*): Normally, if-then rule-based form is set up case by case to describe the relationship between input and output using operators in fuzzy combinations including "and ($\cap$)", "or ($\cup$)" and "not (~)". The fuzzy combinations are also referred to T-norms. In FIS, there are four most common approaches to rule such relations as follows:

1. $\mu_{A\cap B} = \min(\mu_A(x), \mu_B(x))$
2. $\mu_{A\cap B} = \mu_A(x)\cdot\mu_B(x)$
3. $\mu_{A\cup B} = \max(\mu_A(x), \mu_B(x))$ and
4. $\mu_{A\cup B} = \mu_A(x)+\mu_B(x)-\mu_A(x)\cdot\mu_B(x)$

Step 3 (*Defuzzification*): To conclude the FIS process, fuzzy output is reversely transformed to be a single crisp output. There are two most common techniques to tackle with the output distribution, i.e., center of mass and mean of maximum. Based on mathematical combination of the rule strength, the center of mass can be expressed by

$$z = \frac{\sum_{j=1}^{k} z_j \mu_C(z_j)}{\sum_{j=1}^{k} \mu_C(z_j)} \qquad (2.1)$$

where z is the center of mass and $\mu_C(z_j)$ is the membership in class *C* at the value z_j. For mean of maximum, we consider

$$z = \frac{\sum_{j=1}^{k} z_j}{k} \qquad (2.2)$$

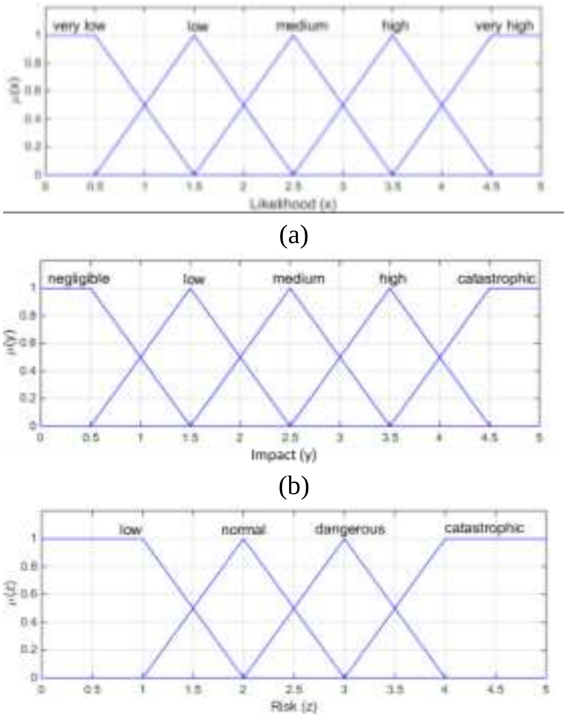
where *z* is the mean of maximum and z_j is the point where the membership function is maximum.

2.3 Modelling fuzzy inference system

Regarding FIS procedure in Section 2.2, fuzzy membership functions of likelihood, impact and risk index are formulated. As shown in Figure 2(a)-(c), $\mu(x)$, $\mu(y)$ and $\mu(z)$ respectively denote the membership functions of the likelihood (*x*), impact (*y*) and risk index (*z*). A membership function is a curve defining how each input variable is mapped to a membership value in the unit interval [0,1]. For simplicity purposes, the triangular membership function is employed to indicate the levels of how each opinion belongs to its linguistic variables and it is defined by

$$\mu_A(x_i : a,b,c) = \begin{cases} 0 & \text{if } x < a, \\ \dfrac{(x_i - a)}{(b-a)} & \text{if } a \le x_i < b, \\ \dfrac{(x_i - b)}{(c-b)} & \text{if } b \le x_i < c, \\ 0 & \text{if } x \ge c. \end{cases} \qquad (2.3)$$

However, membership functions for fuzzy variables do not need to be triangular (Mofarrah & Husain, 2010). Since the membership functions of the input parameters are chosen as triangular distributions, the resulting fuzzy risks have triangular distributions. The degree of likelihood is considered into five different linguistic variables including very low, low, medium, high and very high. The degree of impact is considered into five different linguistic variables including negligible, low, medium, high and catastrophic.



(a)

(b)

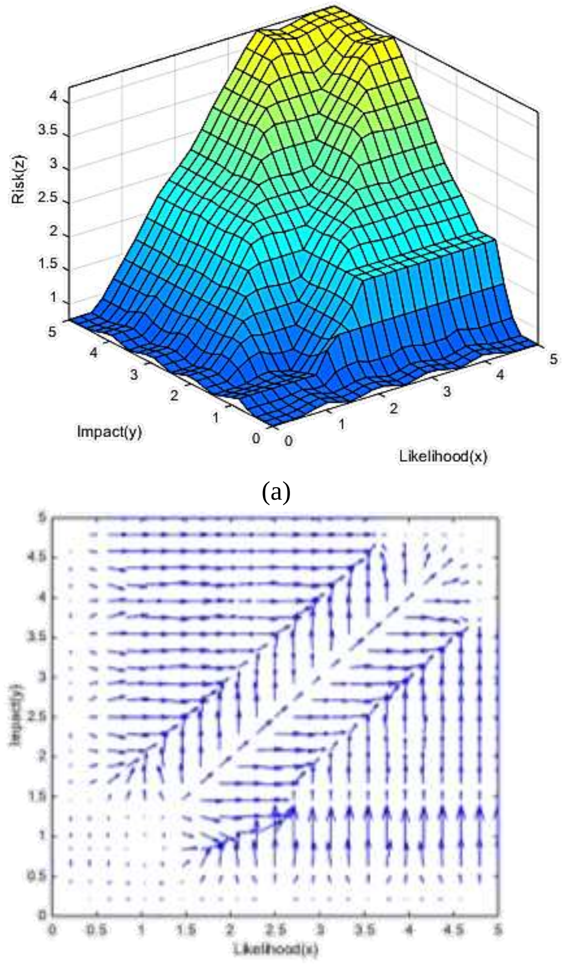
(c)

Figure 2 Membership functions of likelihood, impact and risk

The degree of risk is considered into four different linguistic variables including low, normal, dangerous and catastrophic. We can see that the fuzzy risk matrix is the mapping $X \times Y \to Z$ where *X*, *Y*, *Z* denote likelihood, impact and risk index, respectively. That is, both likelihood and impact have the influence on the level of risk. The conceptualization of fuzzy risk matrix as shown in Figure 3(a) is constructed using centre of mass to represent the mapping from all combinations of two fuzzy inputs (likelihood *X* and impact *Y*) to the fuzzy output (risk *Z*), and its quiver is shown in Figure 3(b).

3. Numerical results

The level of risk index is calculated using two input risk factors, i.e., likelihood and impact. To implement the fuzzy risk assessment, the seriousness degrees of likelihood, impact and risk are scaled into the unit interval [1,0]. After that, the seriousness degrees are defined as fuzzy membership functions of likelihood, impact and risk as shown in Figure 2. Then, 25 if-then rules are carefully constructed by considering the intermediate system parameters and the risk surface in Figure 3(a).

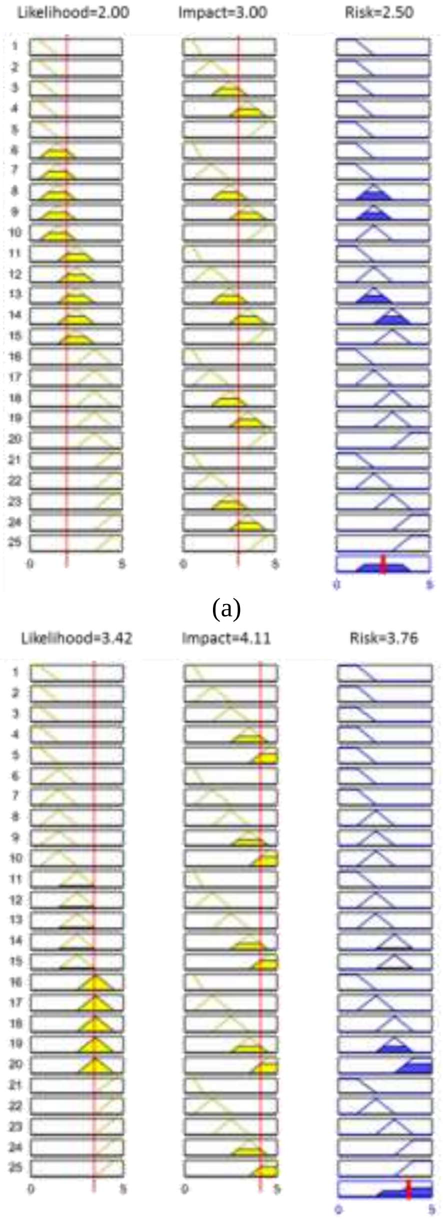


(a)

(b)

Figure 3 Fuzzy risk matrix and its quiver.

As can be seen, Figure 4 exemplifies the risk assessment model from *Fuzzy Logic Toolbox* in MATLAB 2014b. If we enter the dual input (*x* and *y*), we then obtain the risk index (*z*). Regarding risk assessments, the values of risk indices corresponding to all 14 criteria of ISO/IEC 27001:2013 standard are also plotted in radar graphs as displayed in Figure 5. Since the fuzzy risk matrix is the refinement of the classical one, its radar graph is also smoother. After assessing risk by two matrices, it is found that there are five aspects with high risk indices, i.e., management direction for information security, human resource security, physical and environmental security, operations security and information security incident management as presented in Table 1.



(a)

(b)

Figure 4 Examples of Mamdani fuzzy inference involving $(x_i, y_j) = (2,3)$ and $(x_i, y_j) = (3.42, 4.11)$

Table 1 List of criteria with high risk indices

Criteria	% of Agreement	Likelihood	Impact	Classical Risk Index	Fuzzy Risk Index
Management direction for information security	85.71	3.42	3.33	11.39 High	2.89 Dangerous
Human resource security	66.67	3.38	3.38	11.42 High	2.84 Dangerous
Physical and environmental security	76.17	3.30	3.20	10.56 High	2.75 Dangerous
Operations security	71.43	3.11	3.56	11.07 High	3.10 Dangerous
Information security incident management	71.43	3.22	3.44	11.08 High	2.91 Dangerous

4. Conclusion and discussion

4.1 Conclusion

This paper has presented and compared two versions of risk assessments including classical risk and fuzzy logic-based risk assessments from semi-qualitative questionnaires. Advantageously, verbal expressions and linguistic variables of likelihood and impact are usually associated with vague or imprecise identification; so, fuzzy logic is easily accommodated into the risk assessment process. To offer management guideline of operational risk on ICT, the risk criteria have been identified and assessed under ISO/IEC 27001:2013 standard using classical and fuzzy rule-based managements. Based on data analysis in risk assessment, it is found that the case-study organization, Rangsit University, has a high level of risk in five criteria including management direction for information security, human resource security, physical and environmental security, operations security and information security incident management.

4.2 Discussion

A master plan for ICT to initiate policies, measures, rules, regulations and laws should be established to protect innocents, support cyber security and to contribute peace in digital society as all countries have set. Particularly for the case study, its guidelines on risk management can be summarized as follows:

- *Human resource security*

The personnel should strictly comply with the organization's security agreement. The qualifications of all participants should be examined before executing. The personnel must not have a history of compromising, resolving, destroying or stealing information in any department. The organization shall establish disciplinary regulation to punish personnel who violate or break the organization's agreement of ICT security.

- *Management direction for information security*

The organization must establish a security policy for documentary information for directing and supporting the implementation of ICT security systems that respond to corporate mission and organizational policy.

- *Operations risk*

The organization should have a committee to consider and record the damage value, quantity and frequency from intrusion into the system as well as report to the management periodically.

- *Information security incident management*

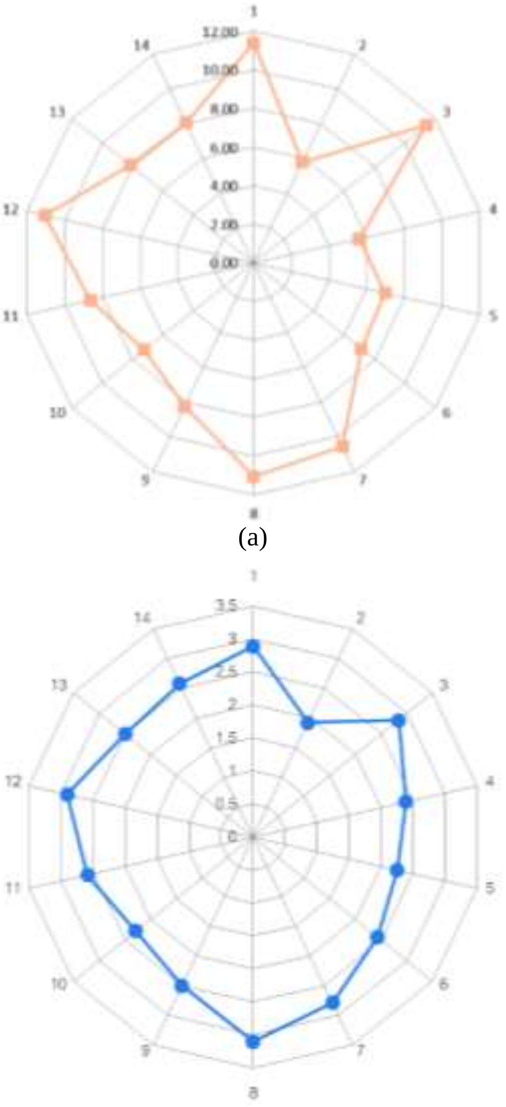
The organization should establish plans or strategies to be able to recover computer system back up and to run normally as soon as possible.

- *Physical and environmental security*

The organization should install fire-fighting equipment such as smoke detectors, heat detectors and sprinkler system to promptly prevent or suppress fire.

The risk management plan should be proposed to executives in the meeting to actually execute for practical use. This is the establishment of a committee to investigate and evaluate the possibility to follow various guidelines as provided in the plan. The organization should officially declare the plan to use and periodically report the results of monitoring mechanism. So, they can measure whether the risk management systems of the organization were effectively and efficiently conducted on targets or not.

1. information security policy
2. organization of information security
3. human resource security
4. asset management
5. assess control
6. cryptography
7. physical and environmental security
8. operations security
9. communication security
10. system acquisition development and maintenance
11. supplier relationship
12. information security incident management
13. information security aspects of business continuity management
14. compliance



(a)

(b)

Figure 5 Risk indices from (a) classical risk matrix and (b) fuzzy risk matrix.

5. Acknowledgements

The authors would like to express gratitude to Asst. Prof. Dr. Somboon Anekritmongkol, Asst. Prof. Dr. Wuttipong Chinnasri and Asst. Prof. Dr. Suttisak Jantavongso for examining content validity, content coverage and the nature of the questionnaire. Many thanks go to Data Centre and Information Technology Service Centre, Rangsit University, Thailand.

6. References

Berg, H. P. (2010). Risk management: Procedures, methods and experiences. *Risk Management*, *1*, 79-95.

Capuder, L. (2004). ISO-7799-Standard for information security: A welcome boon for security management and audit. *EDPACS*, *31*(11), 1-10.

Ciborra, C. (2006). Imbrication of representations: Risk and digital technologies. *The Journal of Management Studies*, *43*(6), 1339-1356. https://doi.org/10.1111/j.1467-6486.2006.00647.x

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, *28*(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Elsayed, T. (2009). Fuzzy inference system for the risk assessment of liquefied natural gas carriers. *Applied Ocean Research*, *31*(3), 179-185.

Groves, S. (2003). The unlikely heroes of cyber security. *Information Management Journal*, *37*(3), 34-40.

Hu, S., Fang, Q., Xia, H., & Xi, Y. (2007), Formal safety assessment based on relative risks model in ship navigation. *Reliability Engineering and System Safety*, *92*, 369-377.

Humphreys, T. (2005). State-of-the-art information security management systems with ISO/IEC 27001. *ISO Management Systems*, 15-18.

Humphreys, E. (2011). Information Security Management System Standards. *Datenschutz und Datensicherheit*, *35*(1), 7-11. DOI: 10.1007/s11623-011-0004-3

Humphreys, E. (2016). Implementing the ISO/IEC 27001:2013 ISMS Standard (2nd Edition). *Artech House*.

Hussey, D .E. (1978). Portfolio analysis: Practical experience with the directional policy matrix. *Long Range Planning*, *11*(4), 2-8. https://doi.org/10.1016/0024-6301(78)90001-8

Karwowski, W., & Mital, A. (1986). Potential applications of fuzzy sets in industrial safety engineering. *Fuzzy Sets and Systems*, *19*(2): 105-120.

Mamdani, E. H., & Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies*, *7*(1), 1-13.

Mansell, R. (1999). Information and communication technologies for development assessing the potential and the risks. *Telecommunications Policy*, *23*(1), 35-50. DOI: 10.1016/S0308-5961(98)00074-3

Markowski, A. S., & Mannan, M. S. (2008), Fuzzy risk matrix. *Journal of Hazardous Materials*, 159, 152-157.

Mofarrah, A., & Husain, T. (2010). Modeling for uncertainty assessment in human health risk quantification: A fuzzy-based approach. *International Congress on Environmental Modelling and Software*, 1-8.

Pinder, P. (2006). Preparing information security for legal and regulatory compliance (Sarbanes-Oxley and Basel II). *Information Security Technical Report*, *11*(1), 32-38. DOI: 10.1016/j.istr.2005.12.003

Philip, T., Bratvold, R., & Bickel, J. E. (2014). The risk of using risk matrices. *SPE Economics & Management*, *6*(2), 56-66.

Ruddock, L. (2006). ICT in the construction sector: Computing the economic benefits. *International Journal of Strategic Property Management*, *10*(1), 39-50. DOI: 10.1080/1648715X.2006.9637543

Segars, A. H., & Grover, V. (1996). Designing company-wide information systems: Risk factors and coping strategies. *Long Range Planning*, *29*(3), 381-392. https://doi.org/10.1016/0024-6301(96)00024-6

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60-66.

Shenkir, W. G., & Walker, P. L. (2006). Enterprise risk management and the strategy-risk focused organization. *Cost Management*, *20*(3), 32-38.

Solms, B. V. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4): 441-469.

Takács, M. (2011). Parameters and rules of fuzzy-based risk management models. *Óbuda Univ. e-Bulletin*, *2*(1), 309-314.

Teneyuca, D. (2001). Organizational leader's use of risk management for information technology. *Information Security Technical Report*, *6*(3), 54-59.

Wu, W., Cheng, G., Hu, H., & Zhou, Q. (2013). Risk analysis of corrosion failures of equipment in refining and petrochemical plants based on fuzzy set theory. *Engineering Failure Analysis*, *32*, 23-34.

Zadeh, L. A. (1973). Outline of a new approach to the analysis of complex systems and decision processes. *IEEE Transactions on Systems, Man, and Cybernetics*, *3*(1), 28-44. DOI: 10.1109/TSMC.1973.5408575.