Journal of System Management (JSM)
Online ISSN: 2538-1571, Print ISSN: 2322-2301
Doi: 10.30495/JSM.2022.1945866.1578
8(1), 2022, pp. 145-166

Received: 26/11/2021
Accepted: 18/01/2022

RESEARCH ARTICLE **Open Access**

Subjectivity Reduction of Qualitative Approach in Information Security Risk Analysis

Alireza Tamjidyamcholo [1*], Abbas Toloie Eshlaghy [2]

Abstract

Qualitative information security risk assessments are somewhat subjective and the high degree of subjectivity associated with the perception of risk means that management is often skeptical of risk analysis results, and is unwilling to make important decisions based on that. Besides, the process of information security risk assessment is quite complex and rife with uncertainty and without taken into account the uncertainty of information security risk assessment the results can be misleading. Therefore, in this paper, the Fuzzy Multi Criteria Group Decision Making (FMCGDM) model is proposed to address the above-mentioned problems. The focus group method used to identify risk parameters and the Delphi method is used to construct a hierarchy for risk parameters. The findings of this research would be useful for the information security department to become more capable in analyzing the InfoSec risks and reducing the consequences of subjective assessment. A case study involving an actual information security risk management project was presented to illustrate the use of the proposed model. Computational results demonstrated the efficiency and effectiveness of the presented model that can assist InfoSec risk analyst to better evaluate InfoSec risk.
Key words: Information Security, Risk Assessment, Qualitative, Subjectivity, Risk Analysis

Introduction

As the information technology industry proceeds with novel technologies and innovations, the information security field remains turbulent and dynamic. Recently, the World Economic Forum revealed that there is interdependence in network infrastructure, and cyber-attacks on this infrastructure are of the world's top risks in 2020 (www.weforum.org). In recent years a few vulnerabilities in the connected cars being reported and it shows that the production of less insecure Internet-of-Things (IoT) devices could build extensive vulnerabilities in cyberspace (www.ics-cert.kaspersky.com). Occurring two destructive ransomware attacks WannaCry and ExPetr changed the perception of industrial enterprises to the problem of securing key production systems. For instance, Ukraine's power distribution systems took down by a cyber-attack and the electricity of 230,000 residents being cut (www.pwc.com). Seeing that more connected devices and vulnerable web applications are deployed in hospitals and several cybersecurity incidents and alerts have seen in healthcare sectors (www.ey.com). Kaspersky Lab reported that cryptocurrencies have created new and unprecedented ways to monetize malicious activity and they claimed about 1.65 million users protected from malicious cryptocurrency miners (https://securelist.com). All the aforementioned evidence proved that the information security field is still challenging

[1,2] Department of Management, Science and Research Branch, Islamic Azad University, Tehran, Iran
* Corresponding Author, Email:itm.tamjid@gmail.com)

and dynamic and needs to be explored and pay special attention to the problems in this subject.

Although the cost of cybercrime may fluctuate by type of cyber-attack, industry, country, organizational size, and maturity and effectiveness of an organization's security posture, the survey conducted independently by Accenture and Ponemon in 2019 shows that the average cost of cybercrime for an organization increased US$1.4 million to US$13.0 million(https://www.accenture.com). Another survey conducted by ISACA shows that the security budgets of organizations are expanding (https://cybersecurity.isaca.org). Elky (2006) from the SANS Institute highlighted that organizations have limited resources and reducing risk to zero levels is almost impossible. Thus, realizing the risks and its magnitude would help organizations to prioritize and allocate wisely their scarce resources. Establishing a systematic and holistic risk planning would be valuable for security and risk efforts, it additionally provides a tool to explain effectively priorities to executive management and the board. In the UK, commonly businesses applying risk assessment concepts to examine their cybersecurity posture and a report from the UK stipulated that 35% of businesses and 27% of charities set out information risk management regimes to improve their cybersecurity (UK, G 2018). Organizations would lose some profit as a consequence of lacking an effective program to manage information security risk. This program can proactively protect enterprise information resources. Therefore, organizations should carry out a sound information security risk management (ISRM) program to attain satisfactory protection of their information assets and reducing the monetary losses; moreover, to comply with the mandatory regulations and governmental laws passed by their society (Fenz & Neubauer, 2018). Wheeler (2011) pointed out that ISRM is an ideal way to systemize the enterprise information security program and can be used as a reporting structure for organization information security posture. Information security risk program needs to be considered as an umbrella term for all the daily activities of information security. NIST 800-100 declared that the important constituent of a successful information security program is an effective risk management process.

Information Security Risk Assessment (ISRA) is the core and critical component in the context of information security risk management. An effective risk assessment can protect organizations against threats and assist organizations to conduct safeguards and controls that are needed. The effectiveness of the risk treatment and making informed decisions about InfoSec investments depends on the results of the risk assessment (ISO/IEC 27005:2018) and it is wise that organizations carry out a proper risk assessment before issuing and implementing information security policies (Eloff & Eloff, 2005). The ISRA approaches can be classified into three main groups: the quantitative approaches, the qualitative approaches, and the combination of both quantitative and qualitative (hybrid) approaches. The usage decision of the qualitative or quantitative approaches is a matter of organizational preference. Most organizations for applying quantitative methods in most cases require historical incident data and the absence of such data on novel risks; additionally, the cost of implementing quantitative approaches encourages specialists to use qualitative approaches. Some advantages of the qualitative assessment include easier to involve nontechnical and non-security staff, uncomplicated calculation, adaptability in reporting and process, simple to understand and not required to assign a monetary value to the asset (Lo& Chen, 2012). Nevertheless, the subjectivity situated in the qualitative risk assessment process is the problem and the high amount of subjectivity related to the perception of risk means that managers in many times is not easily convinced for risk analysis

outcomes, and thus not eager to make important decisions based on that (Brunner, Sauerwein, Felderer, & Breu, 2020; Ryan, Mazzuchi, Ryan, De la Cruz & Cooke, 2012). Furthermore, there is a great deal of uncertainty in the information security domain and managing of this uncertainty has a significant effect on the effectiveness of risk assessment outcomes (Feng & Li, 2011; Alali, et al., 2018). In this paper, the Fuzzy Multi Criteria Group Decision Making (FMCGDM) model proposed to respond to the following research questions: how it can be possible to reduce subjectivity in expert decision-making about the value of information security risk parameters? And how it can be possible to reduce uncertainty placed in the qualitative method of information security risk analysis?

Literature Review

Information security risk management (ISRM) needs two main undertaking: risk identification (assessing risk) and risk treatment (controlling risk) (Whitman, 2018). Risk assessment is defined as a process to examine and record the security condition of an organization's information technology and the risks they confronted (Schmitz & Pape, 2020). Risk control is a process to identify and apply countermeasures to minimize the risks to an organization's information resources and these countermeasures are derived from risk assessment results (Le et al., 2019). If the risk is not identified and assessed properly and timely, it resulted in wrong decision making for controlling risk and security investment decisions (El-Gayar & Fritz, 2010). Several researchers have developed taxonomy for ISRS methods (Pan & Tomlinson, 2016; Zhiwei, Zhongyuan, 2012; Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016; Karabacak & Sogukpinar, 2005). The recent taxonomy published by Shameli-Sendi et al.(2016) concluded that the existing methods for ISRS have two basic challenges. First, the effect of the threat cannot be accurately calculated. Second, the evaluation of the risk is too imprecise. For conducting information security risk assessment, there are three approaches: quantitative and qualitative or a combination of both (Pan & Tomlinson, 2016). Quantitative methods are using mathematical and statistical tools and trying to assign a monetary value to the amount of damage occurring and safeguards' costs. Numerous preliminary works to collect precise values of all risk assessment components is required in the quantitative methods and there is not high-quality historical data for predicting the likelihood of occurrence. In addition, the lack of data for novel threats and vulnerabilities is a problem in the quantitative approach (Brunner, et al., 2020). Furthermore, in quantitative methods some intangibles attributes such as public reputation, brand image and public and customer confidence can be unconsidered (Wangen, 2017). Contrary to quantitative methods, qualitative risk assessment methods are based on intuition, judgment, and experience of risk analysts (Brunner, et al., 2020; Shameli-Sendi et al., 2016) and a large amount of study and plenty of methodologies was based on qualitative method (Schmitz, & Pape, 2020; Sadeghi, Bagheri, Garcia, & Malek, 2016; Yazar, 2002; Conway, Taib, Harris, Yu, Berkovsky, & Chen, 2017). Many professional organizations, like Factor Analysis of Information Risk (FAIR) (https://www.fairinstitute.org/), NIST SP 800-30 (Aroms, 2012); ISO/IEC 27005:2018(www.iso.org); CRAMM (http://www.thecramm.com/); Microsoft's Risk Assessment model (www.microsoft.com); CORAS (http://coras.sourceforge.net/); and the OCTAVE (Alberts & Dorofee, 2002); OCTAVE Allegro (Caralli et al., 2007) and Mehari (www.enisa.europa.eu) proposed methods to ISRA. In addition, some methods for ISRA have been suggested by research projects, an overview of some research that is related to our research briefly explained in the following section. Alali et al., (2018) proposed a model using Mamdani Fuzzy inference

system to produce risk assessment results. Lo and Chen (2012) suggested a hybrid procedure considering interrelations among security control to assess information security risk. Yang, Shieh & Tzeng (2013) defined a model called ISRCAM which revised VIKOR based on DEMATEL and ANP to overcome the problem of interdependence in the information security risk assessment process. A situational fuzzy OWA modeled to select appropriate countermeasures for information security risk reduction (Imamverdiev & Derakshande, 2011). Several studies applied Fuzzy AHP to assess InfoSec risk (Tan& Li, 2012; Peng, & Dai, 2009; Liu et al., 2005; Le et al., 2019), however, neither of professional organizations and academic research methods could present a robust method to reduce the subjectivity of qualitative approach in InfoSec risk analysis.

Qualitative risk analysis is suffering from subjective assessment rather than objective assessment (Brunner et al., 2020; ISO 27005, Feng & Li, 2011). Subjectivity is defined by Cambridge and Longman online dictionary as "A statement, report, attitude, judgment, etc. that is subjective influenced by or based on personal beliefs, opinion or feelings, rather than based on facts and can therefore be unfair" (https://dictionary.cambridge.org). Subjectivity is opposite to objectivity and risk analysis aims to create objective results, not subjective ones. The correctness of the entire qualitative risk assessment model depends on the expert's perception of the risk assessment parameters (El-Gayar & Fritz, 2010). Subjectivity takes place while experts make decisions or heuristic judgments about the value of parameters. Some consequences of subjective assessment include the creation of the wrong posture of security in the organization and result in making inappropriate policy; choosing inappropriate countermeasures to manage risk and limited budget of organization allocated inappropriately (Suh & Han, 2003). Redmill Felix (2002) pointed out that "estimates of risk, whether made by scientists or lay people, cannot escape containing elements of subjectivity, but the neutralization of subjectivity should be considered". This study thus proposed a group decision-making model using the FMCGDM algorithm for handling the subjectivity of assessments and managing the uncertainty and vagueness that remains in the information security risk assessment process.

Fuzzy Multi Criteria Group Decision Making (FMCGDM)

Multiple criteria decision-making (MCDM) techniques presented a procedure for handling complex decision problems. One of the most frequently applied technique for dealing with MCDM problems which is mostly applied in engineering, management and social sciences is the analytic hierarchy process (AHP). AHP is proposed by Saaty in 1970 (Saaty, 1980; Roghani et al., 2021). Evaluations and opinions of decision-makers integrated into AHP and more objectively complex issues can be evaluated by AHP (Lee, 1996). The AHP approach has six essential steps (Intharathirat & Salam, 2020; Proletarsky et al., 2020):1) stating clearly the objective and defining problem.2) the complex problem decomposed and hierarchical structure for decision elements (criteria and alternatives) created.3) Comparison matrices using pairwise comparisons among decision elements formed.4) the decision elements weights by employing the eigenvalue method determined. 5) Consistency test conducted to guarantee that the judgments of decision-makers are compatible. 6) The relative weights of decision constituent aggregated and the final ranking for the alternatives calculated. The standard AHP possesses some deficiency, in particular, there is uncertainty and imprecision in human judgments and decision-making processes (Feng & Li, 2011) and the standard AHP couldn't consider this vagueness and uncertainties. Fuzzy set theory, thus, integrated with AHP to control this problem. Zadeh introduced the fuzzy set theory to cope with the

imprecision and uncertainty, which is inherent to the human judgments in decision making processes, through the use of linguistic terms and degrees of membership (Zadeh, 1979). The triangular fuzzy number and trapezoidal fuzzy number are the two most frequently applied fuzzy membership numbers. A fuzzy number is a fuzzy subset of real numbers whose membership function is $u_M(x): R \rightarrow (0,1)$. The triangular fuzzy number and its membership function are defined as bellow (Lee et al., 2006; Sadathosseini Khajouei & Pilevari, 2021):

$$u_M(x) = \begin{cases} \dfrac{x - m^-}{m - m^-}, & m^- \le x \le m \\ \dfrac{x - m^+}{m - m^+}, & m \le x \le m^+ \\ 0, & Otherwise \end{cases}$$

The m presents the strongest membership grade and $m^-$and m^+indicate the lower bound and the upper bound of the triangular fuzzy number of M respectively; accordingly, the triangular fuzzy number of M is represented by(m^-, m, m^+). The application of fuzzy set theory in a variety of fields has been researched by other academics (Lee, 2010; Mandic et al., 2014; Vahidnia et al., 2009).

In practice, the ISRA is quite complex and full of uncertainty. If the uncertainty and subjectivity of human decision-making are not taken into account in the process of qualitative ISRA, the results could be misleading and the effectiveness of the ISRA significantly would be decreased. Therefore, the authors believe that a combination of fuzzy, AHP and group decision-making, which is named Fuzzy Multi Criteria Group Decision Making (FMCGDM), not only can adequately handle the inherent subjectivity in the human decision-making process but also can control uncertainty and imprecision of ISRA process. Application of FMCGDM in metro system risk assessment and green supplier selection has already been proved in which a combination of fuzzy, AHP and group decision-making can reinforce the reasonableness and comprehensiveness of the decision-making process (Lyu, Sun, Shen & Zhou, 2020; Ecer, 2020). The applied method was firstly introduced by Chang (1992, 1996). The process of this method is less time consuming, less computational expense and relatively easier than many other techniques. The introduced approach is briefly explained here. The two triangular fuzzy numbers contrasted with $M_1(m_1^-, m_1, m_1^+)$ and $M_2(m_2^-, m_2, m_2^+)$. The possibility degree of $V(M_1 \ge M_2) = 1$ is defined when $m_1^- \ge m_2^-,\ m_1 \ge m_2,\ m_1^+ \ge m_2^+$. The possibility degree of $V(M_1 \ge M_2) = 0$ defined when $m_2^- \ge m_1^+$. Otherwise, the possibility degree of $V(M_1 \ge M_2)$ is the ordinate of the highest intersection point between $\mu(M_1)$ and $\mu(M_2)$. $V(M_2 \ge M_1) = hgt(M_{1\cap}M_2) = \mu(d) = \frac{m_1^- - m_2^+}{(m_2 - m_2^+) - (m_1 - m_1^-)}$ where M is a convex fuzzy set, and $\alpha \in [0,1]$ If $x_1 \in M_\alpha$ and $x_2 \in M_\alpha$ then $\mu_M(x_1) \ge \alpha$ and $\mu_M(x_2) \ge \alpha$. μ_α is a closed interval and $x_1 < x < x_2$, so $x \in M_\alpha$ and $\mu_M(x) \ge \alpha = \min(\mu_M(x_1), \mu_M(x_2))$.

Proposed Model

The process of risk analysis initiates with the identification of information assets and carries on with the identification of vulnerabilities rest upon the assets and the threat agents that may exploit the vulnerabilities. As shown in Fig. 1, the well-known studies of Stoneburner, Goguen & Feringa (2002) and Peltier (2005) are adapted to propose the current research risk assessment procedure. The proposed model is structured into four major steps: (1) system characterization (2) vulnerability assessment (3) threat identification and (4) control recommendations. The control recommendation has been omitted in this research and it could be the research subject of other projects.

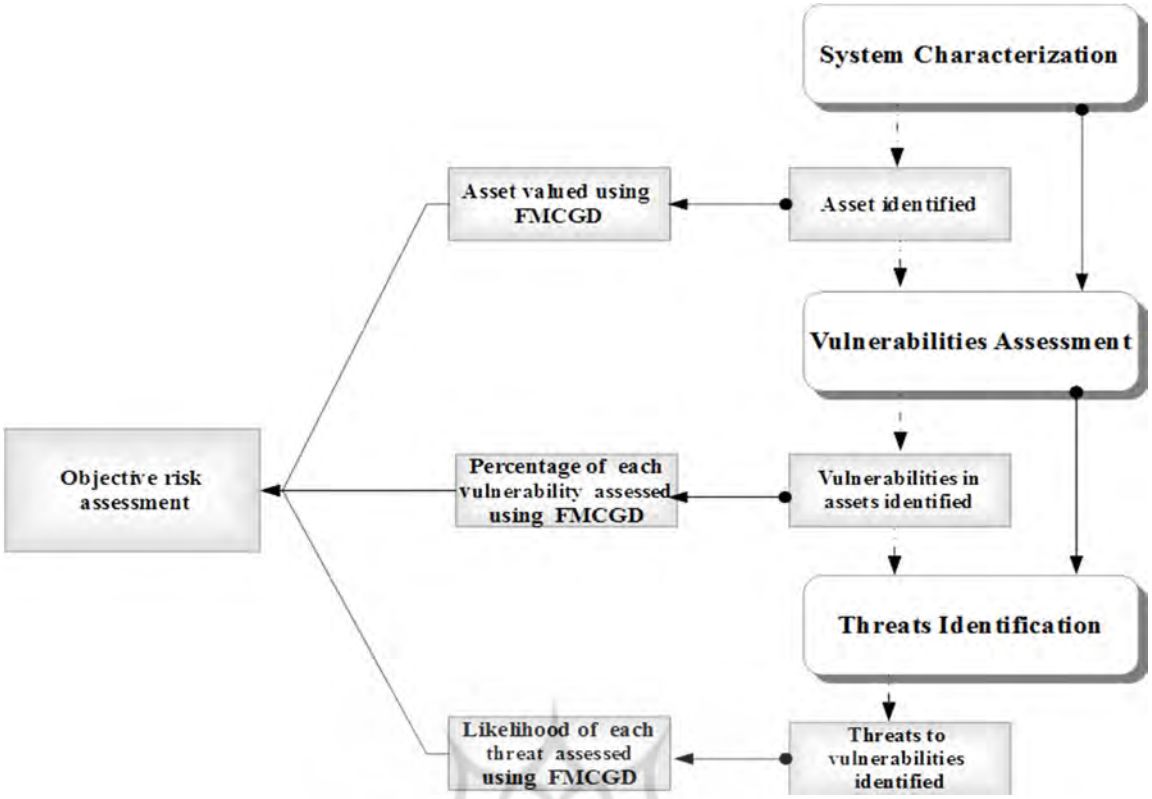

Figure1. Overview of the proposed model

In the first step, the boundaries and the scope of the risk assessments project are defined and characterized. This step provides the analysts with a clear understanding of the entire system and its particularities. The system characterization step output would be a list of assets that their risk should be analyzed. An asset is anything that has value to the organization and therefore requires being protected **(**ISO/IEC 27005:2018**).** The ISO (ISO/IEC 27005:2018) classified assets into two kinds: primary assets and supporting assets. The primary assets are business processes, activities and information. The supporting assets are hardware, software, network, personnel, site and organization's structure. The second step is vulnerability assessments. An excellent definition for vulnerability presented by NIST SP 800-30 and it is defined as a weakness or flaw in system security design, implementation, procedures, or inside controls that could be exploited accidentally or intentionally and concluded a system security policy violation or security breaches in the organization. The goal of this step is to develop a list of system vulnerabilities that could be exploited by potential threat-sources. Landoll & Landoll (2005) categorized the vulnerabilities according to administrative, physical, and technical areas and ISO 27005(ISO/IEC 27005:2018) provided a list of vulnerabilities which is based on threats and asset types. The third step is threat identification. NIST SP 800-30 defined threat as a potential that a threat source or agent accidentally or intentionally could exploit a specific vulnerability. Threats by themselves couldn't take actions, so threats must be mixed with threat agents or sources to create a danger(s) (www.microsoft.com). An entity that may cause the threat to happen is called a threat agent. Possible threat agents can be nature, employees, malicious hackers and industry spies. The outcome of this step is a list of potential threats that could exploit the IT system of the organization. At the end of the

risk identification process, an organization should have a list of assets, threats and vulnerabilities. These lists, as shown in table 1, can be combined into Threats Vulnerabilities Assets (TVA) worksheet. The TVA shows each threat may exploit vulnerability or vulnerabilities which located in each asset. This paper applies the focus group research method to classify assets, to identify vulnerabilities and to extract threats. Focus group research method is based on a selected group of individuals in which the insights and understandings of the group through discussion can be extracted in ways which it is difficult to obtain with simple questionnaire items. Interaction among participants is the key to successful focus group research.

Table 1.
(TVA) worksheet

	⬇Asset 1	Asset 2	……	Asset n
Threat 1 ➡	Vulnerability(s)	Vulnerability(s)	……	……
Threat 2	Vulnerability(s)	Vulnerability(s)	……	
…..	……	……		
Threat n	……	…….		

The focus group members interacted with each other to expose different perspectives through conversation and discourse. In an interactive setting, the reactions of group members spark new ideas in others, and the gap of the discussion may fill with another discussant. Once risk parameters (assets, vulnerabilities and threats) are identified, the value of each component calculated using the proposed FMCGDM method as follows: (1) Define the subjectivity problem in the information security risk assessment process and explain the overall objective. (2) The evaluation criteria for risk parameters (asset evaluation, vulnerability assessment and threat probability) collect via previous research and discussion with people in InfoSec industries and InfoSec experts. (3) The most significant criteria select by the Delphi method. The Delphi method briefly described as follows (Hsu, Lee & Kreng,2010): 3.1 A team to examine the subject sets up, and the experts are the people in the area to be studied; 3.2 the first round of Delphi questionnaire develops; 3.3 the first-round questionnaire's result were sent to the experts and they analyze the responses; 3.4 the second round investigation prepares again with a questionnaire; 3.5 the second round of the questionnaire is transferred to the panelists and they analyze the responses (the two latter steps are repeated until a desire or stability in the results appears); and 3.6 a report of the conclusions present. (4) Based on the selected criteria, a hierarchy for evaluating assets, assessing vulnerability and probability of threats is prepared. (5) A pairwise comparison questionnaire, according to the hierarchy, is produced. The questionnaire is based on a five-point scale. The questionnaire fills out through the invitation of experts. To assure that the expert's opinion is consistent throughout the questionnaire, the pairwise comparison results from each expert are tested. The consistency test (Saaty, 1980) is calculated by the consistency index (CI) and consistency ratio (CR): $CI = \frac{\lambda_{max}-n}{n-1}$, and $CR = \frac{CI}{RI}$ where n is the number of items being compared in the matrix, and RI is the random index. The expert's judgment has consistency if the threshold for consistency (CR <0.1) is obtained. The experts will be required to re-assess the part of the questionnaire if the consistency test is not passed, (6) for criteria i and j, based on each expert's questionnaire outcomes, fuzzy pairwise comparison weights were established. The membership functions of the fuzzy number defined by Table 2.

Table 2.
Membership functions

Fuzzy number	Characteristic(membership) function
$\tilde{1}$	(1,1,2)
$\tilde{x}$	(x-1,x,x+1) for x=2,3,4,5,6,7,8
$\tilde{9}$	(8,9,9)
$1/\tilde{1}$	$(2^{-1},1^{-1},1^{-1})$
$1/\tilde{x}$	$((x+1)^{-1},x^{-1},(x-1)^{-1})$ for x=2,3,4,5,6,7,8
$1/\tilde{9}$	$(9^{-1},9^{-1},8^{-1})$

For an expert, the fuzzy number of *i* and *j* is (p_{ijt}; q_{ijt}; r_{ijt}). (7) Using the geometric mean method, the fuzzy combined pairwise comparison weights for all the criteria were

$$b_{ij}^{-} = \left(\prod_{t=1}^{s} p_{ijt}\right)^{1/s}, \forall \quad t = 1,2,3,\dots,S.$$

$$b_{ij} = \left(\prod_{t=1}^{s} q_{ijt}\right)^{1/s}, \forall \quad t = 1,2,3,\dots,S.$$

$$b_{ij}^{+} = \left(\prod_{t=1}^{s} r_{ijt}\right)^{1/s}, \forall \quad t = 1,2,3,\dots,S.$$

and (p_{ijt}; q_{ijt} ; r_{ijt}) is the comparison weight of criteria i and j from expert t. (8) the consistency of the experts combined opinions and judgment examined. First, using $b_{ij}^{-} = (b_{ij}^{-} + 4b_{ij} + b_{ij}^{+})/6$ (Kwong, & Bai, 2003) the fuzzy geometric pairwise comparison weight of phase seven were defuzzified. Then, the consistency test of the combined opinions of the experts again examined as it is conducted in phase five. (9) The fuzzy synthetic extent value calculated with reference to criterion i:(Chang,1996;Lee,2009): $F_i = \sum_{j=1}^{n} B_{ij} \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{n} B_{ij}\right]^{-1}, \quad i = 1,2,\dots,n \ \ and \ \ j = 1,2,\dots,n$ Where

$$\sum_{j=1}^{n} B_{ij} = \left(\sum_{j=1}^{n} b_{ij}^{-}, \sum_{j=1}^{n} b_{ij}, \sum_{j=1}^{n} b_{ij}^{+},\right) and \left[\sum_{i=1}^{n}\sum_{j=1}^{n} B_{ij}\right]^{-1}$$

$$= \left(1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}^{+},\ 1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij},\ 1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}^{-}\right)$$

$$i = 1,2,\dots,n \quad and \quad j = 1,2,\dots,n$$

calculated. By integrating the experts' judgment, a triangular fuzzy number $\tilde{D}_{ijt}$ is attained. $\tilde{D}_{ij} = (b_{ij}^{-}, b_{ij}, b_{ij}^{+})$ Where

(10) To illustrate the relative importance between two criteria, membership function μ(d) calculated and F_i compared. The possibility degree of a convex fuzzy number to be greater than *K* convex fuzzy number F_K can be determined using(Chang,1996; Lee,2009): $V = F \geq F_1, F_2, \dots, F_k) = \min V(F \geq F_i), \ i = 1,2,\dots,k$; (11) w'_i (the weights of criteria) calculated and w'_i normalized into W. Presume that: $d(F_i) = \min V(F_i \geq F_k) = w'_i (k = 1,2,\dots,n \ \ and \ \ k \neq i)$ the weights of criteria (w'_i)are $W' = (w'_1, w'_2, \dots, w'_n)^T$. The priority weights of criteria, after normalization, are: $W =$

$(w_{1,}w_{2,}\dots,w_n)^T$;(12) Once the weights of criteria determined in level 1, according to each criterion, a pairwise comparison created for each alternative (assets, vulnerabilities, threats) in level 2, then the calculation conducted as step 3 to step 11. The resulted matrix would be:

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \dots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix}$$

(13) The result of hierarchy level one and hierarchy level two multiplied.

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \dots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}$$

(14) The above process was conducted for asset evaluation, vulnerability assessment and threat probability. (15) The results of risk parameters (assets' value, vulnerability percentage and threat probability) multiplied to obtain the risk rate of each asset.

Application of the Proposed Model in a Case Study

A case involving an actual information security risk assessment process was selected to illustrate the credibility of the proposed model. The selected case has around 27000 employees and around 17 departments and sub-departments and working in the education industry and recently being audited to obtain information security, cybersecurity and privacy protection standard (ISO/IEC 27007:2020). More information about the selected organization according to the request could not be shard and is confidential and anonymous. Six domain experts as a decision-making group were formed, the experts were in charge of information security project and had worked on numerous similar information security projects for a minimum of ten years. Two members were from the network and hardware security background, two members were from a software and data security background, and one member was from an IT management background. A suitable level of knowledge and sufficient practical experience are the two main attributes in determining them as field experts. The objectives of the study and data collection and use were explained to the experts before starting the work. Data collection, in this study, is comprised of two steps; first, identification of InfoSec risk parameters which includes identification and classification of assets, listing vulnerabilities in assets and extracting threats to assets by applying focus group research method; second, collecting data to establish FMCGDM for asset valuation, vulnerability assessment and threat occurrence probability.

Relationship between assets, vulnerabilities and threats

A threat is an event or a cause that may harmfully affect an asset (www.microsoft.com). Vulnerability is a lack of control or weakness that rested on an asset and may be exploited by a threat (www.microsoft.com). This paper applies the focus group research method to classify assets, to identify vulnerabilities and to extract threats. After exhaustive discussion with our focus group panels, four important assets identified and twenty-two vulnerabilities which left in assets determined and finally the threats which could exploit the vulnerabilities identified. The connection of assets, threats and vulnerabilities is shown in figure 2.

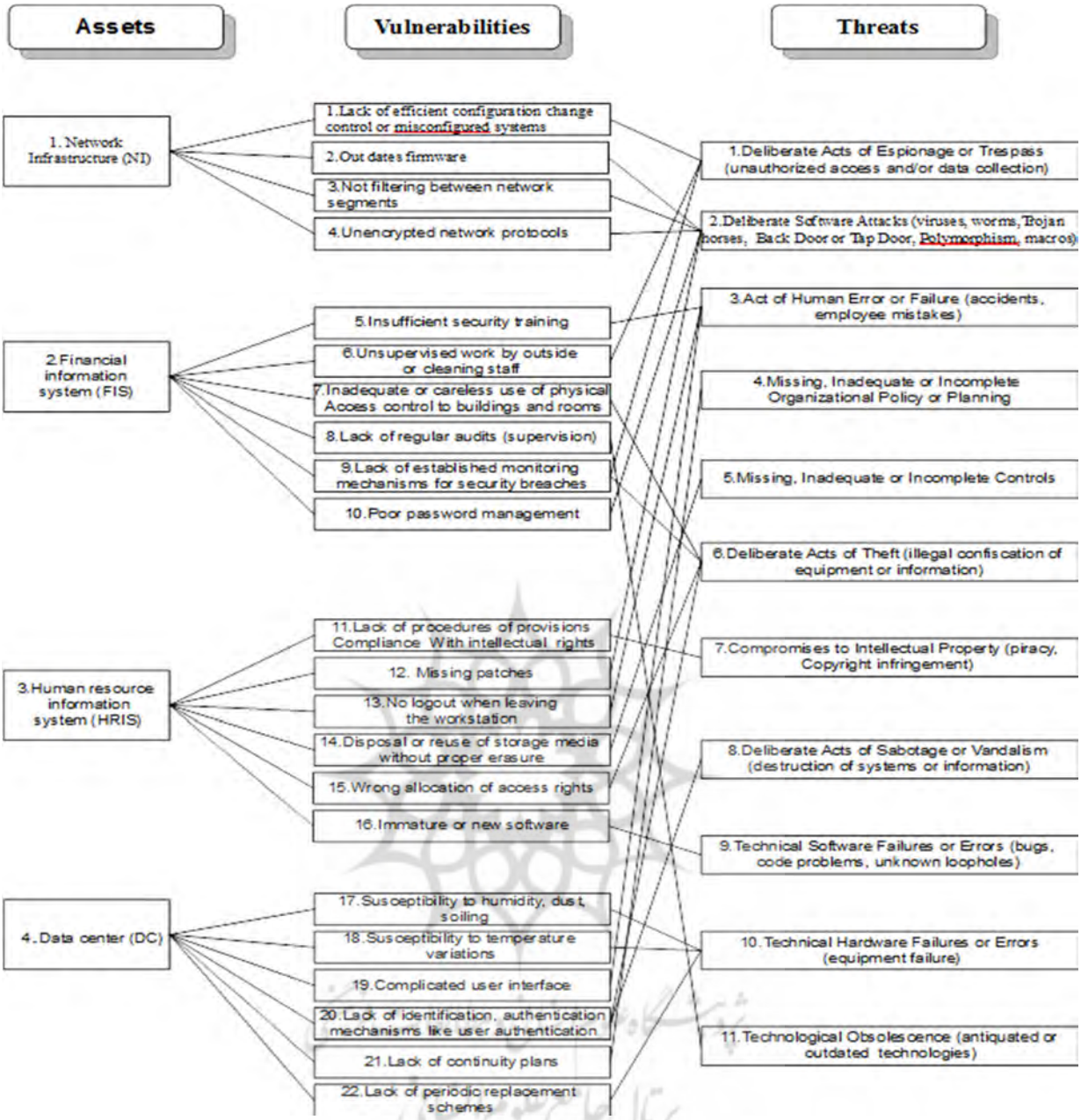

Figure 2. Connection between assets, vulnerabilities and threats

FMCGDM for Asset Valuation

The basic hierarchy of the objective asset valuation was constructed based on the experts' suggestions derived by using the Delphi approach (Heidari, Bavarsad, Nili Ahmad Abadi & Mullah Alizadeh Zavardehi, 2021). In other words, each expert is required to determine feasible elements that could somehow impact the end decision via several discussions, questionnaires and surveys until a consensus is obtained. In addition, based on a critical review of the literature and the discussion process using the Delphi approach applied to obtain the criteria of the hierarchy. As shown in Fig. 3, the top level of the hierarchy denotes the overall objective, namely assessing asset value. The lowest level is the list of assets, viz. network infrastructure,

financial information system, human resource information system, and data center. The three main criteria including confidentiality, availability and integrity are at the middle level.

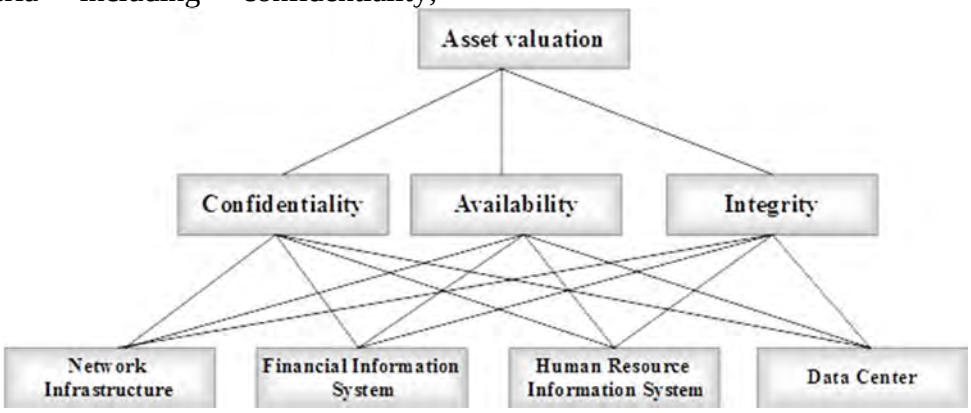

Figure 1. The hierarchy for assets evaluation.

After establishing the hierarchy, the pairwise comparison evaluation takes place. The criteria of the same level are compared to each of the criteria of the upper (preceding) level. Five linguistic terms, "Very Unimportant" (VU), "Less Important" (LI), "Equally Important" (EI), "More Important" (MI) and "Very Important" (VI) is used to perform a pairwise comparison. Based on the hierarchy a questionnaire is constructed. The consistency of the pairwise comparisons of each expert is appraised according to the outcomes of the questionnaires. The consistency index (CI) and consistency ratio (CR) is calculated to examine the consistency. As the CR is less than 0.1, the expert's opinion is consistent and approved. The expert will be required to reconsider the part of the questionnaire if the consistency test is not approved. Once the consistency test of the whole experts for the questionnaire outcomes approved, by applying the definition in Table 2, the fuzzy importance weights of the criteria for each expert are implemented. Next, the fuzzy integrated matrix by combining the data from all the experts is constructed via the geometric mean method. To make certain that the combined opinions even now are consistent, first, the integrated fuzzy matrix is deffuzified and the test of consistency again is executed. Once the consistency is approved, next the fuzzy synthetic extent value in respect of each criterion is calculated. Concerning each criterion, the fuzzy synthetic extent computed and the priorities of the criteria are shown in Table 3.

Table 3.
Calculation of fuzzy synthetic extent, μ (d) and W_i for each criterion

	$\sum_{j=1}^{n} b_{ij}^{-}$	$\sum_{j=1}^{n} b_{ij}$	$\sum_{j=1}^{n} b_{ij}^{+}$	$\sum_{i=1}^{n}\sum_{j=1}^{n} B$	$\left[\sum_{i=1}^{n}\sum_{j=1}^{n} B_{ij}\right]^{-1}$	$1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}^{+}$	$1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}$	$1/\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}^{-}$	μ(d)	W '	W
Confidentiality(F_1)	4.67	5.67	7.67	10	0.1	0.31	0.48	0.77	V(F_1> F_2);1 V(F_1> F_3); 1	1	0.713
Availability(F)	2.53	3.09	3.79	11.8	0.08	0.17	0.26	0.38	V(F_2> F_1);0.24 V(F_2> F_3);0.67	0.24	0.117
Integrity(F_3)	2.81	3.09	3.54	15	0.07	0.19	0.26	0.35	V(F_3> F_1);0.16 V(F_3> F_2);1	0.16	0.169

According to the experts' opinions, the most important criterion is confidentiality, with a priority of 0.713. The next two important criteria are availability and integrity, with priorities of 0.117and 0.169, respectively. A similar procedure is executed to calculate the value of each asset in level 2 of the hierarchy. A combination of experts' opinions for assets concerning each criterion using fuzzy triangular number results is calculated and the calculation of fuzzy synthetic extent concerning criterion F_i and calculation of μ(d)and Wi is computed. In the end, the weights of the assets with respect to the main criteria are combined and the value of the assets is determined. The global preference weights for each asset are calculated by multiplying their criteria weights with preference weights of their respective asset. As indicated in the below matrix, based on the multiplication of level 1 results and level 2 results in a hierarchy, the data center is the most preferred asset with a priority weight of 0.571, followed by financial information system with 0.295 weight and network infrastructure with 0.115 weight, human resource information system with 0.018weight.

$$\begin{bmatrix} 0.041 & 0 & 0.508 \\ 0.354 & 0.328 & 0.022 \\ 0.024 & 0.008 & 0 \\ 0.58 & 0.662 & 0.469 \end{bmatrix} * \begin{bmatrix} 0.713 \\ 0.117 \\ 0.169 \end{bmatrix} = \begin{bmatrix} 0.115 \\ 0.295 \\ 0.018 \\ 0.571 \end{bmatrix}$$

FMCGDM for Vulnerability Percentage Assessment

In this section, we explain how to establish FMCGDM for vulnerability assessment which is proposed in Fig. 1. A similar series of steps executed to calculate asset valuation are applied for vulnerability assessment. The steps of this phase are as follows1) using through Delphi method and discussion and critical literature review six important dimensions, viz. vulnerability to reputation, financial vulnerability, vulnerability to productivity, vulnerability to safety, and health and legal implications of vulnerabilities are determined. 2) according to the identified criteria, as shown in figure 4, a hierarchy for evaluating vulnerability percentage created. 3) A pairwise comparison questionnaire, based on the hierarchy, is designed. 4) The consistency test is calculated and the CR is below than the threshold o.1, thus the test for all the experts successfully passed 5) Fuzzy pairwise comparison weights for criteria *i* and *j* according to the membership functions defined in Table 2 being established. 6) The fuzzy integrated pairwise comparison weights for criteria using the geometric mean method calculated. 7) The fuzzy geometric pairwise comparison weight defuzzified and again the consistency of the integrated opinions of the experts examined and successfully passed. 8) The fuzzy synthetic extent concerning criterion i calculated and μ(d),w'_i and w calculated. 9) Once the weights of criteria are determined in level 1, according to each criterion a pairwise comparison created for each threat in level 2, then the calculation is conducted as step 4 to step 9. It should be considered as indicated in Figure 2 these vulnerabilities rested on the assets, thus the calculation should be separately conducted to each asset. Results of fuzzy synthetic extent with respect to criterion Fi and calculation of μ(d)and Wi for Network Infrastructure (NI), Financial Information System (FIS), Human Resource Information System (HRIS), Data Center (DC) are computed. The network infrastructure vulnerability assessment matrix result is below, i.e., multiplication of level 1 and level 2 in the hierarchy. The percentage of vulnerability for NI is: vulnerability one (0.0889), vulnerability two (0.2239), vulnerability three (0.0845), and vulnerability four (0.216). From FMCGDM perspective, we can understand the first two important vulnerabilities for NI are vulnerability two (out of date firmware) and vulnerability four (unencrypted network protocols). Moreover, the less important vulnerability is vulnerability

three (not filtering between network segments).

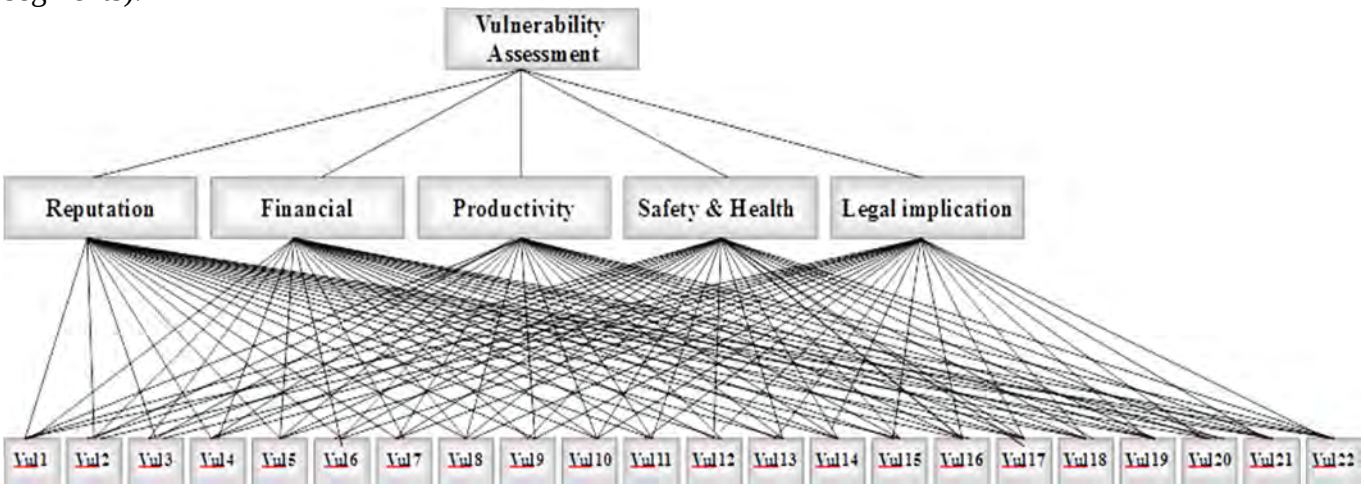

Figure 2. The hierarchy for Vulnerabilities assessment

$$\begin{bmatrix} 0.0179 & 0.4896 & 0.003 & 0.4896 \\ 0.0066 & 0.5048 & 0.0066 & 0.482 \\ 0.2698 & 0.2573 & 0.264 & 0.2089 \\ 0 & 0 & 0 & 0 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix} * \begin{bmatrix} 0.2357 \\ 0.0514 \\ 0.1384 \\ 0.3867 \\ 0.1878 \end{bmatrix} = \begin{bmatrix} 0.0889 \\ 0.2239 \\ 0.0845 \\ 0.216 \end{bmatrix}$$

The resulted matrix for financial information system vulnerability assessment, namely multiplication of level 1 and level 2 illustrated in the below matrix. The percentage of vulnerability from Vul-5(insufficient security training), Vul-6(unsupervised work by outside or cleaning staff), Vul-7(inadequate or careless use of physical access control to buildings and rooms), Vul-8 (lack of regular audit), Vul-9 (lack of established monitoring mechanisms for security breaches) and Vul-10 (poor password management) yield 0.1848, 0.0982, 0.1771, 0.1846, 0.1829 and 0.1722, respectively. Consequently, insufficient security training and lack of regular audit has a highest vulnerability for financial information system asset and unsupervised work by outside or cleaning staff has the lowest percentage of vulnerability for the FIS.

$$\begin{bmatrix} 0.1811 & 0.1085 & 0.1759 & 0.1811 & 0.1811 & 0.1722 \\ 0.1898 & 0.0944 & 0.1668 & 0.1922 & 0.1755 & 0.1813 \\ 0.201 & 0.094 & 0.17 & 0.1793 & 0.1827 & 0.173 \\ 0.1854 & 0.103 & 0.1698 & 0.1998 & 0.1825 & 0.1595 \\ 0.1751 & 0.0798 & 0.202 & 0.1595 & 0.1882 & 0.1954 \end{bmatrix} * \begin{bmatrix} 0.2357 \\ 0.0514 \\ 0.1384 \\ 0.3867 \\ 0.1878 \end{bmatrix} = \begin{bmatrix} 0.1848 \\ 0.0982 \\ 0.1771 \\ 0.1846 \\ 0.1829 \\ 0.1722 \end{bmatrix}$$

Human resource information system vulnerability assessment result matrix is presented in below. Expected vulnerability from lack of procedure of provisions compliance with intellectual rights (Vul-11), missing patches(Vul-12), no logout when leaving the workstation (Vul-13), disposal or reuse of storage media without proper erasure(Vul-14), wrong allocation of access rights (Vul-15) and immature or new software (Vul-16) is 0.14855, 0.04453, 0.08712, 0.1178, 0.07215, and 0.14314 respectively. The percentage of vulnerability from vulnerability 11 and vulnerability 16 has a higher priority.

$$\begin{bmatrix} 0.2554 & 0.06145 & 0.13588 & 0.18812 & 0.15199 & 0.20716 \\ 0.19252 & 0.12148 & 0.13897 & 0.17012 & 0.16833 & 0.20858 \\ 0.18687 & 0.15716 & 0.16213 & 0.20679 & 0.02487 & 0.26218 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0.28002 & 0.01094 & 0.13587 & 0.19223 & 0.12906 & 0.25189 \end{bmatrix} * \begin{bmatrix} 0.2357 \\ 0.0514 \\ 0.1384 \\ 0.3867 \\ 0.1878 \end{bmatrix} = \begin{bmatrix} 0.14855 \\ 0.04453 \\ 0.08712 \\ 0.1178 \\ 0.07215 \\ 0.14314 \end{bmatrix}$$

Datacenter vulnerability assessment results are indicated in the below matrix. Effect of vulnerability 17 (susceptibility to humidity, dust, soiling), vulnerability 18(susceptibility to temperature variations), vulnerability 19 (complicated user interface), vulnerability 20 (lack of identification, authentication mechanism like user authentication), vulnerability 21 (lack of continuity plans), vulnerability 22 (lack of periodic replacement schemes) on DC is 0.2093, 0.0451, 0.0658, 0.01238, 0.2819, 0.2742 respectively. The vulnerability of 17, 21 and 22 has the highest vulnerability percentage.

$$\begin{bmatrix} 0.0979 & 0.0063 & 0.1567 & 0.1908 & 0.2698 & 0.2786 \\ 0.2004 & 0.1487 & 0.0965 & 0.1234 & 0.2368 & 0.1942 \\ 0.1948 & 0.1192 & 0.1726 & 0.0936 & 0.2408 & 0.179 \\ 0.3011 & 0.0355 & 0 & 0 & 0.3317 & 0.3317 \\ 0.1729 & 0.0305 & 0 & 0.317 & 0.2371 & 0.2424 \end{bmatrix} * \begin{bmatrix} 0.2357 \\ 0.0514 \\ 0.1384 \\ 0.3867 \\ 0.1878 \end{bmatrix} = \begin{bmatrix} 0.2093 \\ 0.0451 \\ 0.0658 \\ 0.01238 \\ 0.2819 \\ 0.2742 \end{bmatrix}$$

FMCGDM for Threat Occurrence Probability

Threat probability occurrence using FMCGDM has a similar computational procedure being applied for vulnerability assessment and asset valuation. The procedure is as follows: 1) using through literature review and discussion and the Delphi method four important criteria including the capability of the intruder, motivation of hackers, history of respected threat and effectiveness of current controls are identified. The effectiveness of current controls plays a negative role in our hierarchy. It means that as long as our current control is high and effective, the threat occurrence probability of the respected threat would be lower. 2) Based on the selected criteria, as shown in Fig. 5, a hierarchy for assessing threat probability was created.3) Based on the hierarchy, a pairwise comparison questionnaire is designed 4). The consistency test is performed by calculating the CI and the CR which this test for all experts successfully passed.5) Fuzzy pairwise comparison weights for criteria *i* and *j* according to the membership functions defined in Table 2 being established. 6) The fuzzy integrated pairwise comparison weights for criteria using the geometric mean method calculated. 7) The fuzzy geometric pairwise comparison weight defuzzified and again the consistency of the integrated opinions of the experts examined and successfully passed. 8) The fuzzy synthetic extent concerning criterion i calculated and μ(d),w'_i and w calculated. 9) Once the weights of criteria are determined in level 1, according to each criterion a pairwise comparison created for each threat in level 2, then the calculation is conducted as step 4 to step 9. It should be considered as indicated in Fig. 2 these threats belong to assets, thus the calculation should be separately conducted to each asset. Results of the fuzzy synthetic extent with respect to criterion Fi and calculation of μ(d) and Wi for Network Infrastructure (NI), Financial Information System (FIS), the Human Resource Information System (HRIS), Data Center (DC) calculated. The network infrastructure threat probability assessment matrix result is below (multiplication of level 1 and level 2 in the hierarchy). The threat likelihood for NI is: threat one (deliberate acts of espionage ore trespass) and threat two (deliberate software attacks) has a weight of 0.3876 and 0.6124 respectively. The probability of occurring threat two with considering respected criteria has a double chance in comparison with threat one.

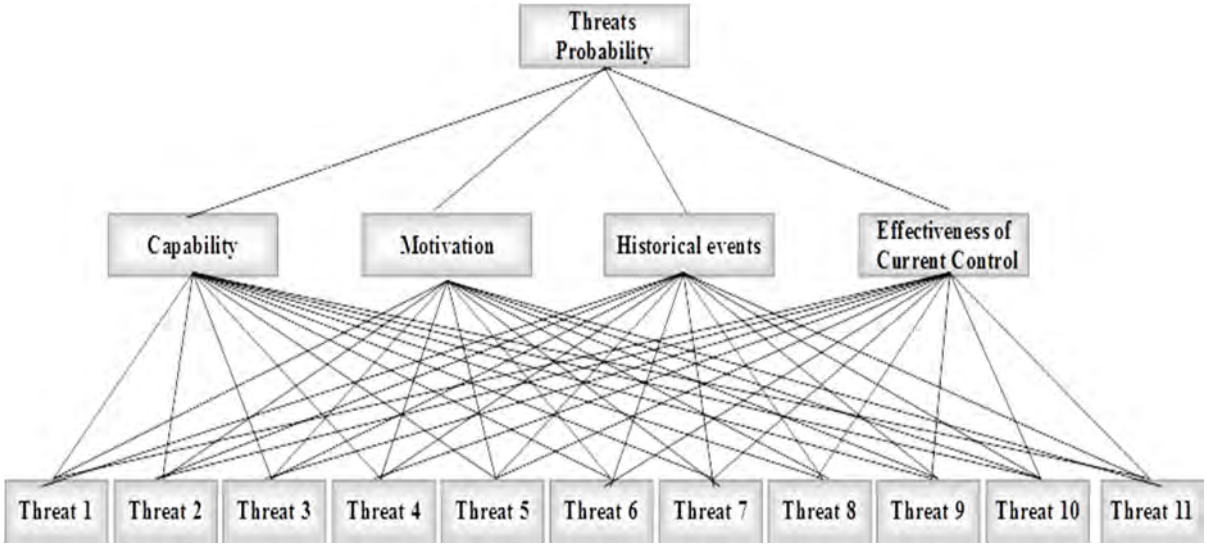

Figure 3. The hierarchy for threats likelihood assessment

$$\begin{bmatrix} 0.3238 & 0.3506 & 0.3067 & 0.59 \\ 0.6762 & 0.6494 & 0.6933 & 0.41 \end{bmatrix} * \begin{bmatrix} 0.2588 \\ 0.2709 \\ 0.2425 \\ 0.2279 \end{bmatrix} = \begin{bmatrix} 0.3876 \\ 0.6124 \end{bmatrix}$$

The below matrix explaining that threat 2 (0.25893) has the highest probability weight to threaten FIS, followed by threat 11(0.22771), threat 1(0.20374), threat 6 (0.11061) and threat 3(0.11061).

$$\begin{bmatrix} 0.16928 & 0.22365 & 0.20962 & 0.21295 \\ 0.18618 & 0.33015 & 0.26641 & 0.24893 \\ 0.20506 & 0.04997 & 0.03554 & 0.15536 \\ 0.20304 & 0.15816 & 0.23006 & 0.20992 \\ 0.23645 & 0.23807 & 0.25837 & 0.17284 \end{bmatrix} * \begin{bmatrix} 0.2588 \\ 0.2709 \\ 0.2425 \\ 0.2279 \end{bmatrix} = \begin{bmatrix} 0.20374 \\ 0.25893 \\ 0.11061 \\ 0.199 \\ 0.22771 \end{bmatrix}$$

As indicated the below matrix Threat 2 (deliberate software attacks) with the probability weight of 0.2456 , Threat 3 (the act of human error or failure) with the probability weight of 0.11924, Threat 5 (missing, inadequate or incomplete organizational policy or planning) with the probability weight of 0.12109, Threat 6 (deliberate acts of theft) with the probability weight of 0.10882, Threat 7 (compromises to intellectual property) with the probability weight of 0.14596, Threat 9 (technical software failures or errors) with the probability weight of 0.25172 threaten human resource information system.

$$\begin{bmatrix} 0.26124 & 0.21692 & 0.19853 & 0.31204 \\ 0.12049 & 0.14944 & 0.15462 & 0.04425 \\ 0.15085 & 0.05679 & 0.14873 & 0.13434 \\ 0.05867 & 0.09627 & 0.11427 & 0.17489 \\ 0.1475 & 0.17489 & 0.14469 & 0.11116 \\ 0.26124 & 0.3057 & 0.23915 & 0.22332 \end{bmatrix} * \begin{bmatrix} 0.2588 \\ 0.2709 \\ 0.2425 \\ 0.2279 \end{bmatrix} = \begin{bmatrix} 0.2456 \\ 0.11924 \\ 0.12109 \\ 0.10882 \\ 0.14596 \\ 0.25172 \end{bmatrix}$$

By referring to the resulted matrix below it is clear that threat 3(act of human error or failure) with the probability of 0.18991, threat 4 (missing, inadequate or incomplete organizational policy or planning)with the probability of 0.18598, threat 6 (deliberate acts of theft)with the probability of 0.18191, threat 8 (deliberate acts of sabotage or vandalism) with the probability of 0.18095 and threat 10(technical hardware failures or errors) with the probability of 0.26124 threaten data center asset.

$$\begin{bmatrix} 0.19895 & 0.22632 & 0.18695 & 0.1395 \\ 0.2251 & 0.19497 & 0.14917 & 0.17006 \\ 0.16127 & 0.15002 & 0.20247 & 0.22138 \\ 0.16127 & 0.14515 & 0.20395 & 0.22138 \\ 0.25341 & 0.28354 & 0.25745 & 0.24767 \end{bmatrix} * \begin{bmatrix} 0.2588 \\ 0.2709 \\ 0.2425 \\ 0.2279 \end{bmatrix} = \begin{bmatrix} 0.18991 \\ 0.18598 \\ 0.18191 \\ 0.18095 \\ 0.26124 \end{bmatrix}$$

Objective Risk Assessment Results

In this research, we apply the most common formula for information security risk assessment. The formula is as follows: Risk= business impact (asset value*vulnerability percentage) *threat probability. Table 4 illustrates the risk assessment result for NI. The overall risk of NI is 4.1%, which 0.38% of this risk resulted from the lack of efficient configuration change control or misconfiguration systems vulnerability and deliberates acts of espionage or trespass threat; 1.58% of the risk belongs to out dates firmware vulnerability and deliberates software attacks threat ; 0.59% of the risk comes from not filtering between network segments vulnerability and deliberates software attacks threat 1.52% of the risk comes from unencrypted network protocols vulnerability and deliberates software attacks threat.

Table 4.
Risk assessment result for NI

Network Infrastructure(NI)				
Asset value	0.1154			
Vulnerability percentage	0.0888(Vul1)	0.2239(Vul2)	0.0845(Vul3)	0.216(Vul4)
Threat probability	0.3876(Thr 1)	0.6124 (Thr 2)	0.6124 (Thr 2)	0.6124 (Thr 2)
Risk rate of NI according to each vulnerability	0.003976(0.38%)	0.01583(1.58%)	0.005977(0.59%)	0.015273(1.52%)
Overall risk of NI	0.041056312(4.1%)			

Table 5 shows FIS risk evaluation result. The aggregate risk of FIS is 6.97%, this risk comes from insufficient security training vulnerability and the act of human error or failure threat, unsupervised work by outside or cleaning staff vulnerability and deliberate acts of espionage or trespass threat, inadequate or careless use of physical access control to building and rooms vulnerability and deliberate acts of theft threat, lack of regular audits vulnerability and technological obsolescence threat, lack of established monitoring mechanisms for security breaches vulnerability and deliberates acts of espionage or trespass plus deliberate acts of theft threat, poor password management vulnerability and deliberate software attacks threats with 0.6%,0.59%,1.04%,1.24%,2.17%,1.32% respectively.

Table 5.
Risk assessment result for FIS

Financial information system(FIS)						
Asset Value	0.2952					
Vulnerability percentage	0.1848(Vul-5)	0.0982 (Vul-6)	0.1771 (Vul-7)	0.1846 (Vul-8)	0.1829 (Vul-9)	0.1722 (Vul-10)
Threat Probability	0.1106(Thr-3)	0.2037 (Thr-1)	0.199 (Thr-6)	0.2277 (Thr-11)	0.2277 (Thr-1 + Thr-6)	0.2589(Thr-2)
Risk rate of FIS according to each Vulnerability	0.0060(0.6%)	0.0059(0.59%)	0.0104(1.04%)	0.0124(1.24%)	0.0217(2.17%)	0.0132(1.32%)
Overall risk of FIS	0.069679916(6.97%)					

As it is shown in Table 6 lowest risk belongs to HRIS. Lack of procedures of provisions compliance with intellectual rights vulnerability and compromises to intellectual property threat(0.04%), missing patches vulnerability and deliberate software attacks threat (0.02%), no logout when leaving the workstation vulnerability and act of human error or failure threat(0.02%), disposal or reuse of storage media without proper erasure vulnerability and missing, inadequate or incomplete controls threat(0.02%), wrong allocations of access right vulnerability and deliberate acts of theft threat and immature or new software vulnerability and technological software failures or errors threat created 0.185% risk rate for HRIS.

Table 6.Risk assessment result for HRIS

Human resource information system(HRIS)						
Asset Value	0.0183					
Vulnerability percentage	0.1485(Vul-11)	0.0445(Vul-12)	0.0871(Vul-13)	0.1178(Vul-14)	0.0721(Vul-15)	0.1431(Vul-16)
Threat Probability	0.14596 (Thr-7)	0.2456 (Thr-2)	0.1192 (Thr-3)	0.1211 (Thr-5)	0.1088 (Thr-6)	0.2517(Thr-9)
Risk rate of HRIS according to each Vulnerability	0.0004(0.04%)	0.0002(0.02%)	0.0002(0.02%)	0.0002(0.02%)	0.0001(0.01%)	0.0006(0.06%)
Overall risk of HRIS	0.00184884(0.185%)					

In this research, the highest risk resulted from DC with a 14.15% risk rate (Table 7). Susceptibility to humidity dust, soiling vulnerability and technical hardware failures or errors threat with 3.12% risk rate, susceptibility to temperature variations vulnerability and technical hardware failures or errors threat with 0.67% risk rate ,complicated user interface vulnerability and act of human error or failure threat with 0.71% risk rate, lack of identification, authentication mechanism vulnerability and deliberate acts of thefts threat plus deliberate acts of sabotage or vandalism threat with 2.56% risk rate, lack of continuity plan vulnerability and missing, inadequate or incomplete controls threats with 2.99% risk rate, lack of periodic replacement schemes vulnerability and technical hardware failures or errors threat with 4.09% risk rate are the origins of DC risk.

Table 7. Risk assessment result for DC

Data Center(DC)						
Asset Value	0.5710					
Vulnerability percentage	0.2092(Vul-17)	0.0450(Vul-18)	0.0658(Vul-19)	0.1238(Vul-20)	0.2818(Vul-21)	0.2742(Vul-22)
Threat Probability	0.2612 (Thr-10)	0.2612 (Thr-10)	0.1899 (Thr-3)	0.180953(Thr-6+Thr-8)	0.18598 (Thr-4)	0.2612 (Thr-10)
Risk rate of DC according to each Vulnerability	0.0312(3.12%)	0.0067(0.67%)	0.0071(0.71%)	0.0256(2.56%)	0.0299(2.99%)	0.0409(4.09%)
Overall risk of DC	0.1415 (14.15%)					

Conclusion

In this paper, we presented an FMCGD model to reduce subjectivity in the qualitative approach of ISRA. The focus group method for an anonymous company applied first to identify risk parameters including assets,

vulnerabilities, and threats. Then, the relationship between these parameters was determined; it means which threat could exploit the vulnerability situated in the identified asset(s). The Delphi method is applied next to construct a hierarchy for assets valuation, vulnerability assessment and threat probability estimation. Three main attributes for asset valuation, five important dimensions for vulnerability assessment, and four major criteria for threat probability estimation are identified based on the literature survey and the experience of the experts in the information security department. A Comparison of the main attributes and risk parameters are made using questionnaires. Fuzzy sets theory is used to overcome the uncertainty of the ISRA process. The weights of the main attributes and risk parameters are examined using the fuzzy AHP calculation method. A case study involving an actual information security risk management project was presented to illustrate the use of the proposed model. Computational results demonstrated the efficiency and effectiveness of the presented model that can assist InfoSec risk analyst to better evaluate InfoSec risk assessment. The findings of this research would be useful for the information security department to become more capable in analyzing the InfoSec risks and reducing the consequences of subjective assessment. Furthermore, this approach provides a more accurate, effective, and systematic decision support tool. As this paper is the first one that introduces a model to address the subjectivity problem in ISRA process, there are several opportunities for future research. For future research, the authors suggest the list of introduced criteria and alternatives in the case study may not be inclusive. Thus, one may comprise more criteria and alternatives, establish more hierarchies to consider the problem in more detail. Furthermore, the model provides a structured and systematic approach to effectively assessing InfoSec risk. This study, therefore, may be extended to incorporate different areas of risk assessment such as financial and insurance risk assessment. Additionally, the researcher could use the other multicriteria techniques including fuzzy TOPSIS and ELECTRE III to assess InfoSec risk and compare their result with the current research model.

References

Aroms, E. (2012). NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems.

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc..

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323-339. https://doi.org/10.1016/j.cose.2017.09.011

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. Computers & Security, 101776. https://doi.org/10.1016/j.cose.2020.101776

Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP. European journal of operational research, 95(3), 649-655. https://doi.org/10.1016/0377-2217(95)00300-2

Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., & Chen, F. (2017). A qualitative investigation of bank employee experiences of information security and phishing. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 115-129).

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012). Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Ecer, F. (2020). Multi-criteria decision making for green supplier selection using interval type-2 fuzzy AHP: a case study of a home appliance manufacturer. Operational Research, 1-35. https://doi.org/10.1007/s12351-020-00552-y

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10-16.

https://doi.org/10.1016/S1361-3723(05)70275-X
El-Gayar, O. F., & Fritz, B. D. (2010). A web-based multi-perspective decision support system for information security planning. Decision Support Systems, 50(1), 43-54. https://doi.org/10.1016/j.dss.2010.07.001
Elky, S. (2006). An introduction to information systems risk management.
Fenz, S., & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. Information & Computer Security.
Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 11(7), 4332-4340 https://doi.org/10.1016/j.asoc.2010.06.005
Hsu, Y. L., Lee, C. H., & Kreng, V. B. (2010). The application of Fuzzy Delphi Method and Fuzzy AHP in lubricant regenerative technology selection. Expert Systems with Applications, 37(1), 419-425. https://doi.org/10.1016/j.eswa.2009.05.068
Heidari, S., Bavarsad, B., Nili Ahmad Abadi, M., & Mullah Alizadeh Zavardehi, S. (2021). Identifying and Prioritizing Supply Chain Sustainability Indicators for Perishable Products Via Grounded Theory and Fuzzy Hierarchical Analysis Approach. Journal of System Management, 7(1), 233-264. 10.30495/jsm.2021.1919814.1427
Imamverdiev, Y. N., & Derakshande, S. A. (2011). Fuzzy OWA model for information security risk management. Automatic Control and Computer Sciences, 45(1), 20-28 https://doi.org/10.3103/S0146411611010056
Intharathirat, R., & Salam, P. A. (2020). Analytical Hierarchy Process-Based Decision Making for Sustainable MSW Management Systems in Small and Medium Cities. In Sustainable Waste Management: Policies and Case Studies (pp. 609-624). Springer, Singapore. https://doi.org/10.1007/978-981-13-7071-7_55
Kwong, C. K., & Bai, H. (2003). Determining the importance weights for the customer requirements in QFD using a fuzzy AHP with an extent analysis approach. iie Transactions, 35(7), 619-626.
Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. Computers & Security, 24(2), 147-159. https://doi.org/10.1016/j.cose.2004.07.004
Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.
Lee, A. H. (2009). A fuzzy AHP evaluation model for buyer–supplier relationships with the consideration of benefits, opportunities, costs and risks. *International Journal of Production Research*, *47*(15), 4255-4280
Lo, C. C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 39(1), 247-257. https://doi.org/10.1016/j.eswa.2011.07.015
Lo, C. C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, *39*(1), 247-257. https://doi.org/10.1016/j.eswa.2011.07.015
Liu, F., Dai, K., Wang, Z., & Ma, J. (2005, April). Research on fuzzy group decision making in security risk assessment. In *International Conference on Networking* (pp. 1114-1121). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-31957-3_127
Le, A., Chen, Y., Chai, K. K., Vasenev, A., & Montoya, L. (2019). Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats. *Mobile Networks and Applications*, *24*(5), 1713-1721. https://doi.org/10.1007/s11036-018-1047-6
Lee, H. M. (1996). Group decision making using fuzzy sets theory for evaluating the rate of aggregative risk in software development. Fuzzy sets and Systems, 80(3), 261-271. https://doi.org/10.1016/0165-0114(95)00201-4
Lyu, H. M., Sun, W. J., Shen, S. L., & Zhou, A. N. (2020). Risk assessment using a new consulting process in fuzzy AHP. Journal of Construction Engineering and Management, 146(3), 04019112.
Lee, S. H. (2010). Using fuzzy AHP to develop intellectual capital evaluation model for assessing their performance contribution in a university. Expert systems with applications, 37(7), 4941-4947. https://doi.org/10.1016/j.eswa.2009.12.020
Mandic, K., Delibasic, B., Knezevic, S., & Benkovic, S. (2014). Analysis of the financial parameters of Serbian banks through the application of the fuzzy AHP and TOPSIS methods. Economic Modelling, 43, 30-37.

https://doi.org/10.1016/j.econmod.2014.07.036
Proletarsky, A., Berezkin, D., Popov, A., Terekhov, V., & Skvortsova, M. (2020). Decision Support System to Prevent Crisis Situations in the Socio-political Sphere. In Cyber-Physical Systems: Industry 4.0 Challenges (pp. 301-314). Springer, Cham.
Peltier, T. R. (2005). Information security risk analysis. CRC press.
Pan, L., & Tomlinson, A. (2016). A systematic review of information security risk assessment. International Journal of Safety and Security Engineering, 6(2), 270-281. 10.2495/SAFE-V6-N2-270-281
Peng, X., & Dai, F. (2009, May). Information systems risk evaluation based on the AHP-fuzzy algorithm. In 2009 International Conference on Networking and Digital Society (Vol. 2, pp. 178-180). IEEE. 10.1109/ICNDS.2009.124
Redmill, F. (2002). Risk analysis-a subjective process. Engineering Management Journal, 12(2), 91-96. 10.1049/em: 20020206
Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. Computers & Operations Research, 39(4), 774-784
https://doi.org/10.1016/j.cor.2010.11.013
Roghani, M., Modiri, M., Fathi Hafshjani, K., & Alirezaei, A. (2021). Futurology of Multi-Criteria Decision Making Techniques Using Philosophical Assumptions of Paradigms in Scenario Writing. Journal of System Management, 6(3), 139-168. 10.30495/jsm.2021.678899
Sadeghi, A., Bagheri, H., Garcia, J., & Malek, S. (2016). A taxonomy and qualitative comparison of program analysis techniques for security assessment of android software. IEEE Transactions on Software Engineering, 43(6), 492-530 10.1109/TSE.2016.2615307
Sadathosseini Khajouei, M., & Pilevari, N. (2021). Application of Adaptive Neuro-Based Fuzzy Inference System to Evaluate the Resilience of E-learning in Education Systems, During the Covid-19 Pandemic. Journal of System Management, 7(3), 1-34. 10.30495/jsm.2021.1939375.1518
Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. Computers & Security, 90, 101656. https://doi.org/10.1016/j.cose.2019.101656
Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. Information & Management, 41(2), 149-158. https://doi.org/10.1016/S0378-7206(03)00044-2
Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 800-30.
Saaty, T. L. (1988). What is the analytic hierarchy process? In Mathematical models for decision support (pp. 109-121). Springer, Berlin, Heidelberg.
Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & security, 57, 14-30. https://doi.org/10.1016/j.cose.2015.11.001
Tan, Z., & Li, P. (2012). Group decision-making information security risk assessment based on AHP and information entropy. Research J. of Applied Sciences, Engineering and Technology, 4(15), 2361-2366.
UK, G. (2018). Cyber security breaches survey 2018
Vahidnia, M. H., Alesheikh, A. A., & Alimohammadi, A. (2009). Hospital site selection using fuzzy AHP and its derivatives. Journal of environmental management, 90(10), 3048-3056. https://doi.org/10.1016/j.jenvman.2009.04.010
Wheeler, E. (2011). Security risk management: Building an information security risk management program from the Ground Up. Elsevier.
Whitman, M. (2018). Challenges in the Instruction of Risk Management.
Wangen, G. (2017). Information security risk assessment: a method comparison. Computer, 50(4), 52-61.
Yazar, Z. (2002). A qualitative risk analysis and management tool–CRAMM. SANS InfoSec Reading Room White Paper, 11, 12-32.
Yang, Y. P. O., Shieh, H. M., & Tzeng, G. H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 232, 482-500 https://doi.org/10.1016/j.ins.2011.09.012
Zadeh, L. A. (1979). Fuzzy sets and information granularity. Advances in fuzzy set theory and applications, 11, 3-18.
Zhiwei, Y., & Zhongyuan, J. (2012). A survey on

the evolution of risk evaluation for information systems security. Energy Procedia, 17, 1288-1294. https://doi.org/10.1016/j.egypro.2012.02.240

Web references

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
https://www.iso27001security.com/html/27005.html
https://www.iso.org/standard/75281.html
https://www.fairinstitute.org/
http://www.thecramm.com
https://www.microsoft.com/en-us/cybersecurity/content-hub/risk-management-for-cybersecurity-security-baselines
http://coras.sourceforge.net/
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html
https://dictionary.cambridge.org/dictionary/english/subjectivity?q=Subjectivity+