International Journal of Safety and Security Engineering
Vol. 10, No. 2, April, 2020, pp. 161-174
Journal homepage: http://iieta.org/journals/ijsse

A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment

Davor Maček[1,2*], Ivan Magdalenić[1], Nina Begičević Ređep[1]

[1] Faculty of Organization and Informatics, University of Zagreb, Pavlinska 2, Varaždin 42000, Croatia
[2] UniCredit Services GmbH, Vienna 1020, Austria

Corresponding Author Email: davor.macek@foi.hr

https://doi.org/10.18280/ijsse.100202

Received: 12 January 2020
Accepted: 26 March 2020

Keywords:
information security, multicriteria decision making, risk assessment methods, systematic literature review

ABSTRACT

In today's fast, agile, complex and interconnected business world, one of the main goals and concerns is to find an efficient and effective way of managing information security risks. So, one of the means is usage of multicriteria decision-making techniques for such purposes. The vast majority of research begins with some form of literature review. Thus, the review of the literature must be done thoroughly and impartially in order to obtain certain scientific value. This paper provides a systematic literature review (SLR) of relevant and recent literature from both research domains, namely information security risk management and multicriteria decision-making, identifying the standards, methods, techniques and tools that are considered to be the most relevant in the research areas observed. The main purpose of the paper is to discover complementary ISRA and MCDM methods that could be used as a basis to create a new hybrid model for more efficient evaluation of critical IT solutions. The related context, main goals, review methods, relevant results of each research phase along with the findings, papers' analysis, recommendations and conclusions are all given in this review article in order to fully comply with the SLR requirements.

1. INTRODUCTION

Risks have different dimensions and effects with the ability to occur at different levels and require their own specific preventative measures at any level [1]. Today, there is no organization that is not facing with certain security threats (e.g. malware, ransomware, phishing, eavesdropping, impersonating, denial of service, etc.) and consequently related risks to their information systems. Among the most significant risks to which all the organizations today are exposed to are IT operational risks arising from inadequately established internal processes, people and systems, or from negative external events, such as natural disasters or computer attacks on resources [2]. Thus, the risk management is recognized as a key component of managing IT security risks [3]. There are many various definitions of risk set by different international organizations and standards, i.e. ISO/IEC 27005 [4], ISO Guide 73:2009 [5], COSO [6] or NIST SP 800-30 [7]. The focus in this paper is actually on the risk assessment which is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires very careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [7]. Risk assessment is considered to be the most important and critical ISMS (Information Security Management System) planning phase in the risk management process itself [8], which ensures that risks are within acceptable limits given the level of risk appetite defined by senior management. The first step in the process of conducting an information security risk assessment (ISRA) is to clearly define and understand the approach that will be used in the process itself, and there are two possible approaches: qualitative and quantitative [9].

Quantitative risk analysis is used to assign monetary and numerical values to all elements of the risk analysis process. All elements within the analysis were quantified and entered into the equation to determine the total and residual risk. Since this type of risk assessment is very complex, time consuming, expensive and overall difficult to conduct entirely, it's rarely used in practice as a standalone approach, but it's usually combined with qualitative approach. On the other hand, qualitative risk analysis is based on the subjective judgments of information security risk assessment team members to determine the overall risk to information system. Qualitative methods go through different scenarios for risk probabilities and threat severity rankings and for evaluation of possible countermeasures. Qualitative assessment methods include judgments, best practice, intuition, and the experience of the assessor. In qualitative risk analysis, there are no numerical values, but the risk is ranked on a hierarchical scale, e.g. Critical, High, Medium and Low. One of the fundamental ways to adequately manage information security risks lies in choosing the appropriate method for this purpose. Not all risk analysis and risk assessment methods are suitable for all the purposes and all the cases. So, in this survey, the focus is on the application of qualitative risk assessment methods.

The main objective of information security and all business decision makers is to protect the organization itself and the ability to protect the associated IT assets, as well as to ensure the confidentiality, integrity and availability of information and information systems that receive, process, store and

distribute such information, and securing the organization's resources [10]. The complexity of the decision-making process depends on the complexity of the problem defined. Deciding on the level of risk to an information system and selecting appropriate security countermeasures or IT solutions is usually a very complex and demanding process due to insufficient amount of information and resources along with time constraints in organizations. That's why this process can be considered as a multicriteria decision-making (MCDM) problem.

This paper provides a Systematic Literature Review (SLR) of relevant and recent literature on the usage of information security risk management (ISRM) and multicriteria decision-making fields, identifying the standards, methods, techniques and tools that are considered to be the most relevant in the research areas observed. The paper is organized according to SLR Guidelines [11] where detailed context and objectives are given in Introduction and Background chapters respectively, review methods are described in Methodology section, then the results with details of all research phases and relevant findings are in Results section. Analysis of papers along with discussion and recommendations are provided in Analysis and discussion section. At the end, the conclusion along with identified open issues and certain plan for the future research in observed domains is also provided.

2. BACKGROUND

The main objective of this paper is to systematically select and review published literature on ISRA and MCDM fields, and present an overview of the existing and possible further approaches, particularly when combining risk assessment methods along with MCDM techniques in order to make certain evaluations of IT security risks and eventually critical IT solutions by using ISRA elements as evaluation criteria.

2.1 ISRA methods

One of the most important conducted researches of relevant ISRA standards, methods and tools, was ENISA (European Network and Information Security Agency) survey as it provided a precious documentation [12, 13] of previously known methods and standards for managing and assessing information security risks. ENISA survey has been also used as a starting point for research on ISRA methods in some other studies [14, 15] and can be considered as a relevant source. The purpose of ENISA's research was to identify outstanding issues in the field of information security risk management and to provide a roadmap for addressing further outstanding issues at European level. Also, it should be added that the ENISA public web site offers the possibility of comparing many ISRA / ISRM standards, methods and tools [16] with one another according to certain common criteria and characteristics, which can, in a very simple and effective way, identify the advantages and disadvantages of each. So, every organization can choose the method that best suits its needs and business goals. The ENISA repository thus represents the most important reference point in the analysis of ISRA methods. Anyhow, certain drawback of ENISA repository is that it's not updated with the most recent ISRA standards, methods and tools. ENISA is European Union agency for cybersecurity that was established in 2004. The Agency works closely together with the EU Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities, e.g. to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. ENISA counterpart in the U.S. would be CISA (Cybersecurity and Infrastructure Security Agency) within the Department of Homeland Security. CISA builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies [17].

Other relevant sources of knowledge on the application of ISRA methods, which are also based on a systematic review of the literature, include the following studies:

- *Taxonomy of information security risk assessment* (*ISRA*) [18]: A taxonomy has been created for information security risk assessment from as many as 125 papers published from 1995 till May 2014. ISRA methods are divided into professional organizations on the one hand and research projects on the other.
- *A Systematic Review of Information Security Risk Assessment* [19]: A systematic review of the literature was made with 80 papers found on the topic of information security risk in the period 2004-2014. The classification of the works themselves and the ISRA methods was done.
- *Risk Management in Information Security: A Systematic Review* [20]: A systematic review of the main bibliographic databases was conducted with the main research question set *What are the methodologies and methods to manage RIS* (*Risks of Information Security*)?

2.2 MCDM methods

Techniques for supporting in decision-making process can be identified from 3 perspectives [21]:

1. Multicriteria Decision Making, MCDM
2. Mathematical Programming, MP
3. Artificial Intelligence, AI.

From a systematic review of literature on the application of decision-making techniques, and considering the purpose of this scientific survey, only MCDM techniques will be considered that can be classified into 4 following categories [21]:

1. Multi-attribute utility methods (MAUT), e.g. AHP and ANP
2. Outranking methods, e.g. ELECTRE, PROMETHEE and QUALIFLEX [22]
3. Compromise methods, e.g. TOPSIS and VIKOR
4. Other MCDM methods, e.g. SMART [23], DEMATEL and SAW [24].

A short description of the most significant MCDM methods follows:

The most well-known MAUT method is the Analytic Hierarchy Process (AHP). In the AHP the decision-making problem is decomposed into a hierarchy. At the top of the hierarchy is the decision-making goal. The criteria are on the next level and can be decomposed into the sub-criteria. On the last level are the alternatives. By using pairwise comparisons and judgments of decision maker(s), local priorities of

alternatives as well as criteria weights are calculated. Then, it is possible to calculate the total priorities of alternatives and make decision [25]. In the decision-making problem field, if influences/dependencies exist between criteria, using the Analytic Network Process (ANP) is more appropriate. The decision-making problems in the ANP are modeled as networks, not as hierarchies as with the AHP. The ANP is a generalization of the AHP. The basic elements in the hierarchy and network are clusters, nodes and dependencies (arcs). By using the ANP, we can model the dependencies and feedback between the decision-making elements [26], and calculate more precise weights of the criteria as well as the local and global priorities of alternatives.

ELECTRE is an outranking method developed to choose the best action from a given set of actions. It was applied to three main problems: choosing, ranking and sorting. There are two main parts to an ELECTRE application: first, the construction of one or several outranking relations, which aims at comparing in a comprehensive way each pair of actions; second, an exploitation procedure that elaborates on the recommendations obtained in the first phase. The nature of the recommendation depends on the problem being addressed: choosing, ranking or sorting. Usually ELECTRE is used to discard some alternatives to the problem, which are unacceptable [27].

PROMETHEE method is most useful where groups of people are working on complex problems, with several multi-criteria, involving a lot of human perceptions and judgments, whose decisions have long-term impact. It provides the decision maker with both complete and partial rankings of the actions [28].

TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) is based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution [29].

VIKOR method is developed to solve decision problems with conflicting and non-commensurable criteria, assuming that compromise is acceptable for conflict resolution, the decision maker wants a solution that is the closest to the ideal, and the alternatives are evaluated according to all established criteria. VIKOR ranks alternatives and determines the solution named compromise that is the closest to the ideal [30].

DEMATEL is widely accepted as one of the best methods for modeling influences between components. In the decision-making field, it is used to form and then analyze relationships between criteria [31].

There are indeed numerous books and other relevant sources on MCDM methods and techniques, and at least the following are examined to get the basic knowledge and references on it for the purpose of this survey:

- *Application of decision-making techniques in supplier selection: A systematic review of literature* [21]: This scientific research paper provides a systematic overview of decision making support techniques and proposes their classification.
- *Mathematical foundations of the methods for multicriterial decision making* [32]: This scientific paper describes the mathematical foundations for some of the most significant methods for multicriteria decision making, i.e. AHP, ELECTRE, PROMETHEE and TOPSIS methods.
- *Multiple Attribute Decision Making: Methods and Applications* [33]: In this book, the authors explain in detail the issues of multicriteria decision-making as well as the most important methods and their applications.
- *Multi-criteria Decision Analysis: Methods and Software* [34]: The book describes decision problems along with structured MCDA methods in relation to the problem domain (choice, ranking, sorting and description problems). Also, some specialized software solutions were presented to support multicriteria decision-making.

Both of the research domains, ISRA and MCDM, are very attractive for today's researchers and since the ultimate goal of this research is to find relevant scientific articles where certain MCDM methods are applied for the purpose of IT security risk assessment and analysis, thus in the following sections the methods used, results obtained, along with the necessary paper analysis and conclusions will be presented.

3. METHODOLOGY

In this research, the literature review from scientific bibliographic databases was approached by applying guidelines for systematic literature review (SLR) in software engineering proposed by authors B. Kitchenham and S. Charters [11]. SLR is a formalized and repeatable process for documenting relevant knowledge in a particular research area. It's actually a form of secondary study that uses a well-defined methodology to identify, analyze and interpret all available evidences related to a specific research question in a way that is unbiased and (to a degree) repeatable. SLR review methods of data sources and search strategy, study selection and study quality assessment are given in this chapter.

The main objective of this research is to find out what ISRA and MCDM methods and techniques are used together to evaluate and rank security risks to information systems.

The systematic review of the literature was done in 3 consecutive phases:

1. An overview on the application of the most significant ISRA / ISRM methods and standards
2. An overview on the application of the most important MCDM methods and techniques
3. The literature review on the application of MCDM methods in the area of IT security risks.

The SLR process started by identifying the relevant research question for each of the phases (defined and described in section *4. Results*). The decision was that our research should be focused on scientific databases rather than specific books or journals. The following electronic databases were selected for this review:

- Web of Science Core Collection, https://www.webofknowledge.com/
  - Search categories:
    - Phase 1: Computer Science, Information Systems, and Telecommunications
    - Phase 2: Operations Research, Applied Mathematics and Management
    - Phase 3: Operations Research, Applied Mathematics, Management, Computer Science and Telecommunications

- Document types: Article, Proceedings paper
- Limitation: first 10 pages of results (10 results per page)
- Sort: by relevance

- IEEE Xplore Digital Library, https://ieeexplore.ieee.org/
  - Content types: Conferences, Journals
  - Limitation: first 4 pages of results (25 results per page)
  - Sort: by relevance

- ScienceDirect, https://www.sciencedirect.com/
  - Article type: Research articles
  - Limitation: first 4 pages of results (25 results per page)
  - Sort: by relevance

- Google Scholar, https://scholar.google.com/
  - Limitation: first 10 pages of results (10 results per page)
  - Sort: by relevance

- SpringerLink, https://link.springer.com/
  - Content types: Conference paper, Article
  - Discipline: Computer Science
  - Limitation: first 5 pages of results (20 results per page)
  - Sort: by relevance.

These citation databases were chosen because of their provision of important and high impact full text journals and conference proceedings. The selected scientific databases have very good coverage of papers related to ISRA and MCDM topics.

In order to find all relevant studies from citation databases, the inclusion and exclusion criteria were set up:

- Papers written only in English and published in a scientific journal or presented at a scientific conference (proceedings) are included
- Papers need to relate to a research questions regarding the evaluation and application of ISRA and MCDM methods
- Book chapters, encyclopedias, patents, news, discussions, briefs, software publications, videos, and other types of non-relevant articles are excluded
- Emphasis is placed on primary research papers and therefore other review papers are excluded
- Duplicate papers found in more than one citation database were counted only once when calculating the occurrence or representation of an ISRA and/or MCDM method/standard/technique
- Papers not explicitly related to the topic of analysis, assessment and treatment of information security risks, and in which some of the ISRA and/or MCDM methods have not been analyzed or applied, are excluded
- Papers found with Notice of Retraction indication have not been reviewed, i.e. these are excluded due to unknown reasons for the retraction
- Critical criterion for inclusion in statistics: the analysis of the ISRA and MCDM method/standard itself and/or its application in the reviewed scientific work or research was mandatory, not just referencing in the text to some ISRA or MCDM method/standard
- Timeframe for papers publication:
  - Phase 1 and phase 2: 2006 – 2018
  - Phase 3: 2012 – 2018. The reason to shorten the time period of published articles is to find only the most recent papers where MCDM methods are applied for the purposes of information security risk assessment and analysis.
- In order for a particular paper related to ISRA and MCDM to be selected, it must satisfy all of the inclusion and exclusion criteria specified.

The following search queries with Boolean operators (AND, OR) were used for each of the survey phase:

Phase 1:
("Information Security Risk") AND ("Management" OR "Assessment" OR "Analysis") AND ("Standards" OR "Methods" OR "Methodology" OR "List" OR "Comparisons")

Phase 2:
("Multiple-criteria") AND ("Decision") AND ("Making" OR "Method" OR "Technique" OR "Analysis" OR "Comparison")

Phase 3: it's based on the outcome of phase 1 and phase 2, the adequate search query will be created (it's provided in phase 3 part of the Results section).

One of the difficulties in this research on the application of ISRA and MCDM methods we faced was the necessity to check entirely and in details the vast majority of the papers found in citation databases search in order to be able to make relevant statistics and conclusions. Thus, all the papers found in a survey had to be analyzed in details, since the basic overview of the title, abstract, keywords and conclusions in most of the papers were not sufficient enough to find out what all the ISRA and MCDM methods, techniques, standards and tools were actually used and analyzed in a single article. To perform such labor intensive activities, a lot of time and resources were required.

The major disadvantage of SLR is that it requires considerably more effort than traditional literature reviews. The limitation of the chosen SLR methodology lies in its rigor. Some of the promising researches were not selected in the final statistics and review analysis because all the rigorous defined criteria were not completely satisfied. Also, the additional limitations of the SLR guidelines is that the impact of the research questions on the review procedures in not considered, nor the mechanisms needed to perform meta-analysis are specified in detail. According to the analysis of the SLR methodology in software engineering provided in the paper [35], SLR is useful and could be used to decrease the biases and to increase the review quality. Also, it's important that the scope of the review should be limited by choosing clear and narrow research questions. The SLR methodology can be considered as a standard for conducting the literature review in the field of information sciences, and thus was chosen for this research.

4. RESULTS

In this section, SLR Guidelines [11] were followed by clearly indicating review questions in each phase of the research, along with review methods of data extraction and

data synthesis, and finally the necessary results' findings and related description details with graphs are provided.

4.1 Phase 1: An overview of ISRA methods

The Phase1 actually has the aim to show the application of ISRA methods and standards in scientific researches, not just practical use in the IT / IT Security industry. The research question based on the defined main objective of this research and related to the literature review for ISRA / ISRM standards and methods is the following:

- *Which methods, standards, and tools for analyzing and assessing information security risks are the most significant, or most commonly evaluated and applied in practice and used in scientific research*?

Thus, for this Phase 1, the research was approached as follows:

1. An overview of the most important industry standards and methods in the field of information security risk management.
2. An overview of scientific literature from relevant databases on the topic of information security risk assessment and risk management.

The first point has been already addressed by examining ENISA survey and was followed by the systematic survey of ISRA methods, standards and techniques. The survey found that there is currently an extremely large number of methods, techniques and tools and a relatively small number of industry standards for information security risk analysis, assessment and management. In papers where multiple ISRA methods were analyzed or used (which was actually the most common case), the incidence was reported and counted separately for each method. Thus, given the defined search strategy and the parameters for inclusion and exclusion, a total number of 91 relevant papers were found on the topic of information security risk analysis, assessment and management.

The survey discovered that the international industry standard ISO/IEC 27005 (with different release years) was dominantly analyzed and used for the purposes of information security risk analysis, assessment, treatment and management.

It should be also noted that papers referencing the ISO/IEC 27001 standard in the context of the risk analysis and risk assessment method were not considered for counting the occurrence of this standard, since ISO/IEC 27001 is nevertheless primarily used to build an information security management system (ISMS), while an ISO/IEC 27005 standard from the ISO 2700x series is specifically designed for analyzing, assessing, treatment and managing information security risks. Also, in some older scientific papers analyzing or referencing the ISO/IEC 13335-1 standard from 2004, the incidence was anyhow counted for ISO/IEC 27005, since ISO/IEC 13335-1 was replaced by the aforementioned newer standard from the series ISO 2700x.

Apart from the listed information security risk analysis standards and methods in Table 1, the search found also some other ISRA methods that were explored in certain papers, but with little lower frequency of use, e.g. OWASP Risk Rating Methodology, FRAP, CobIT 5 for Risk, FAIR, FMEA, TARA, MITRE, Microsoft Security Risk Management Guide, etc. These mentioned ISRA methods are also very appreciated and valuable in information security world.

Table 1. Frequency of use of ISRA standards and methods

ISRA / ISRM standard or method	Frequency of ISRA / ISRM analysis and applications in papers
ISO 27005	54
OCTAVE	44
NIST SP 800-30	36
CORAS	28
CRAMM	27
ISO/IEC 31010:2009	17
MEHARI	12
AS/NZS 4360	11
EBIOS	11
MAGERIT	11
BSI IT-Grundschutz	10

4.2 Phase 2: An overview of MCDM methods

The research question based on the defined main objective of this survey and related to the literature review for MCDM techniques is the following:

- *Which methods, techniques and tools for multicriteria decision-making problems are the most commonly evaluated and applied in scientific research*?

For the Phase 2, the MCDM methods were surveyed for the most common disciplines related to the application of MCDMs itself (i.e. Operations Research, Applied Mathematics and Management) in the most prominent electronic citation databases that were available to the authors during the research.

The literature survey showed, as indicated in Table 2, that there is a significant number of methods, techniques and tools used to solve multicriteria decision-making problems, with the predominant use of AHP and TOPSIS methods (and their fuzzy variants) being almost equally represented.

In calculating the incidence of analysis and application of a MCDM technique in scientific papers, the same principle was used as when survey of ISRA methods was conducted. So, the main criterion when reviewing statistics for inclusion was whether any MCDM method or technique was merely referenced in the text or literature, or the same technique has really been analyzed and applied as a tool to solve a particular problem of multicriteria decision-making. Papers in which some MCDM technique was only referenced or mentioned in the literature review, but without analysis or concrete application of the same MCDM technique, were not included in this statistic of the calculated papers.

Table 2. Frequency of use of MCDM methods

MCDM methods and techniques	Frequency of MCDM analysis and applications in papers
TOPSIS	71
AHP	70
PROMETHEE	30
ELECTRE	29
VIKOR	26
ANP	17
SAW	12
DEMATEL	10
QUALIFLEX	9
SMART	5

Thus, given the defined parameters of inclusion and exclusion of the papers and the search strategy, a total number of 140 relevant papers from citation databases were found related to the problem of multicriteria decision-making on a relatively small sample. It is also important to note that when subcategories emerged for certain MCDM techniques used in some studies, the occurrence was counted for the main technique within the observed MCDM family. For example, fuzzy AHP and fuzzy TOPSIS techniques, fuzzy extended AHP technique (FEAHP) and fuzzy ELECTRE and fuzzy PROMETHEE versions did not have separate statistics, but such techniques were grouped according to the parent family of a particular MCDM technique. This is done just to simplify the presentation of results.

This survey found that also some other MCDM techniques were examined and applied in certain papers, but with very low representation, such as aggregation methods (ARAS, WASPAS, SWARA, MOORA, MULTIMOORA and COPRAS), Social Choice, GAIA elimination method (Geometric Analysis for Interactive Aid), and MACBETH and LINMAP as methods for multi-attribute group decision-making.

4.3 Phase 3: An application of MCDM methods in information security risk assessment field

The third phase of this literature survey is actually the most important because it integrates the findings from the previous two phases to provide a cross-section of mutual applications of ISRA and MCDM standards, methods and techniques. At this stage of the literature survey, the goal to obtain a cross-section of research areas, that is, to see how the most important multicriteria decision-making methods and techniques are used for the purposes of analysis, assessment, treatment and general management of information security risks.

The research question based on the defined main objective of this survey and related to the literature review for cross-section of the application of ISRA and MCDM methods is the following:

- *Which methods, techniques and tools for multicriteria decision-making problems are the most commonly evaluated and applied in scientific researches for the purpose of risk assessment and management*?

The following search query with Boolean operators (AND, OR) was used in order to search index citation databases:

("Information" OR "Security") AND ("Risk Management" OR "Risk Assessment") AND ("AHP" OR "ANP" OR "TOPSIS" OR "VIKOR" OR "ELECTRE" OR "PROMETHEE")

It's also important to add as when searching ScienceDirect citation database with the above mentioned search query, then search engine limitation occurred with the following indication: Search does not support more than 8 Boolean connectors per field. But anyhow it did not affect the results of the survey, and it was assured by conducting simple tests by removing one of the OR operators from the search query.

For this third survey phase, ACM Digital Library citation database was additionally included in order to make the research more comprehensive and accurate. Only 2 relevant papers were found in ACM Digital Library [36, 37].

4.4 Findings

A review of the literature shows as there is indeed a significant application of relevant MCDM methods and techniques in the context of risk assessment for various social, engineering or medical fields. E.g., risks of software projects, selection of cloud services, customer relationship management, construction projects, selection of various suppliers, then risks of rail, maritime and transport systems, security of the water supply system, nuclear power plants, health systems, outsourcing of e-procurement services, credit risks, etc. But, a relatively smaller number of relevant works were found that relate specifically to the analysis and assessment of information security risks by using MCDM techniques in combination with some ISRA method or ISRA elements.

Figure 1 shows that the predominantly used MCDM technique for the purposes of IT security risk analysis is the AHP, which is attributable to the relative ease of application of the AHP itself and its great popularity among researchers. The search found a total number of 65 relevant papers published at conferences or scientific journals that meet the search criteria and answer the research question. The complete list of all selected studies is [1, 36-99]. Of those 65 papers, 27 papers were published in scientific journals and 38 works are presented in conference proceedings.

The inclusion criteria for the papers' selection and analysis were impact factors of the prominent journals (e.g. Expert Systems with Applications, Computers & Security, etc.) and database citations, along with the necessary relevancy to the topic of application of MCDM in the information security risk assessment field.

In Figure 2, there can be seen the trends of publishing relevant papers related to mutual inclusion of both observed domains. More than 60 papers selected for this SLR with very rigorous criteria defined show certain popularity of the application of MCDM for the purposes of information security risk analysis with the prediction of further growth in research.

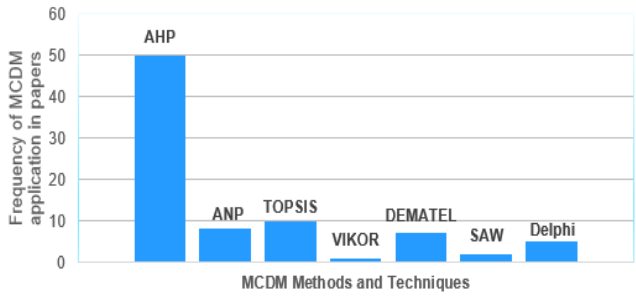

Figure 1. Application of MCDM techniques for the purpose of analyzing and assessing risks to an information system

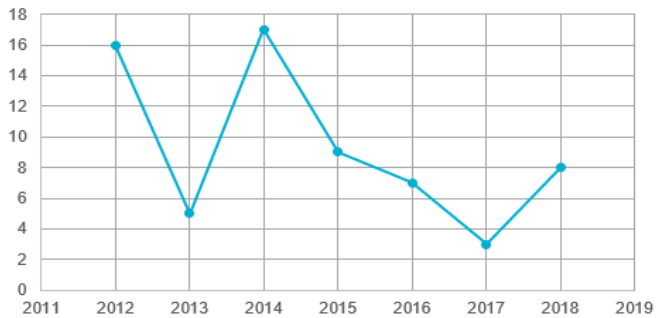

Figure 2. Number of selected studies per year

5. ANALYSIS AND DISCUSSION

In this section, according to the SLR Guidelines, we will present the analysis of the results, i.e. primary studies, and discussions with related strengths and weaknesses of the survey, meanings of findings (for planned further research) and structured recommendations for the usage of MCDM methods in the field of information security risk management.

5.1 Analysis of papers

Below, the most important papers identified through the research of the relevant literature will be presented and briefly analyzed where the application of MCDM methods for the purpose of information security risk assessment has been observed. In the following analysis, the most important works are grouped and analyzed by specific thematic units, e.g. standard risk assessment factors, BCM, cloud security, critical systems, security incidents, etc.

The newly proposed models are created for dealing with security controls:

According to the study [38], a hybrid procedure is proposed for more efficient evaluation of the level of risk to information systems, taking into account the interrelated interdependencies between security controls combining the DEMATEL technique and the ANP. Yang et al. [39] propose a hybrid ISRCAM model (Information Security Risk-Control Assessment Model) that combines as many as 3 MCDM techniques (VIKOR, ANP and DEMATEL) to address conflicting criteria with interdependence and feedback. This model should help IT and security managers to understand the control areas or goals that need to be improved in order to get aligned with the acceptable level of risk (i.e. residual risk) per organization. Using the DEMATEL network relations map (NRM) technique, the proposed model can help to analyze why certain security controls have more deficiencies (vulnerabilities). The risk management model is necessarily a continuous process based on the PDCA (Plan-Do-Check-Act) strategy, so in this study the proposed ISRCAM model examines the effectiveness of controls in the so-called "Check" phase. These 2 works are very imporant because of use of the DEMATEL technique to map interdependencies between security elements. Authors *N. Al-Safwani et al.* in their research combine the ISRA standard ISO/IEC 27005 with the TOPSIS technique to improve the assessment of implemented information security controls [40], and later on they propose an ISCP (Information Security Control Prioritization) model for selection of critical security controls [41]. The TOPSIS method was integrated in the Identification of Existing Controls step during the risk analysis and identification process within the ISO/IEC 27005 risk management framework. The TOPSIS technique was used to determine and rank critical and vulnerable information security controls within a company's IT department based on 5 evaluation criteria, namely known vulnerabilities, valid vulnerabilities, attack class, severity of attacks, and remediation effort level. Critical controls against these criteria were evaluated by experts in Vulnerability Assessment and Penetration Testing (VAPT) field. The main purpose of the model is actually to reduce the over-spending of resources in terms of cost and time and to optimize the assessment of security controls themselves.

These articles are grouped according to the use of standard risk assessment factors in created models:

Zhang and Shao [42] clearly identifies 4 risk assessment factors, namely information assets, threat to property, vulnerability and existing (implemented) security countermeasures. Also, the AHP model for classification of information assets is presented, taking into account the already mentioned risk assessment factors as evaluation criteria, but the paper does not specify to which exact information systems the proposed model would be applied and no necessary (inherent) interdependencies defined between risk assessment factors (which is actually a drawback of the AHP itself). Lee [43] proposes identical risk analysis factors as in the paper [42], except that for each of the 4 criteria in the AHP certain additional sub-criteria are also defined. E.g. CIA attributes for assets, environment and human threat factors, etc. Also, Tianshui and Gang in the paper [44] clearly defines the basic elements for risk assessment (asset, threat, vulnerability) together with the related categories (e.g. data, software, hardware, attacks on the network environment, etc.), but unlike [42, 43] also considering the impact relationships between the elements of risk assessment and the uncertainty created by the security and privacy risk assessment process itself, and thus proposes a new security and privacy risk assessment model for an information system based on DEMATEL method and the ANP combined with a gray system theory.

The analyzed papers are related to BCM (Business Continuity Management):

Hiete et al. in their paper [45] use DEMATEL technique for the purpose of analyzing the structure of complex cause and effect relationships between disaster vulnerability sub-indicators. The paper is important in the context of the impact of a potential disaster on the information system and, above all, disaster resilience, implying the availability of information system as one of the three most important security attributes (the C-I-A triad). The element of resilience is quite often neglected and its importance is not sufficiently emphasized in assessing the security status of an information system, so the significance of this research actually follows. Kim and Na in their paper [46] propose TOPSIS method for systematic risk assessment with interval data to address the recovery problems of critical business processes, i.e. prioritizing them during a business interruption incident, for the purpose of BCM. Access frequency, access time, alternative work time, Recovery Time Objective (RTO) and loss amount were used as evaluation criteria.

In the proposed models, the CIA (Confidentiality, Integrity, Availability) attributes are used as evaluation criteria:

In papers [47, 48], the AHP is used for risk assessment with two-tier criteria for evaluating alternatives, using C-I-A security attributes as the first level criteria as fundamental factors influencing second-tier criteria for evaluating alternatives. Kim [49] proposes the AHP model also with CIA criteria for evaluating and ranking security controls, defined according to the standard NIST SP 800-53 [50], that are necessary for implementation to assess security risk and adequately protect social networking systems (Facebook, Twitter, LinkedIn, etc.). CIA attributes are well-known and the most used elements in security evaluations when impact to information systems needs to be assessed.

The proposed models and methods are related to cloud computing systems:

Li and Bardi [100] propose a model for the evaluation of 4 characteristic risk-inducing factors for cloud computing, namely assets, vulnerability, threat and control measures,

which have been assessed using the AHP and multi-level fuzzy evalution. Zhu et al. [51] further propose a holistic multilevel model of an index system for assessing cloud computing security using the *Delphi* method and the AHP. In addition, Fan and Chen [52] proposed a strategy for assessing cloud computing risk using the *Delphi* technique for structuring key risk factors (criteria) and the ANP for defining the interdependence and impact between defined criteria and sub-criteria as well as the necessary calculations of their weights. In doing so, privacy is indicated as the most significant risk factor. On the other hand, Alguliyev and Abdullayeva [53] proposed a method for dynamic federation of cloud entities based on risk assessment using the AHP, where the basic idea is to avoid the need to initiate the trust between different entities that want to associate together for the sake of ad hoc joining a federation. The proposed method seems to be quite revolutionary, but also difficult to apply in a corporate environment (especially in financial institutions) because of the very context of cloud computing, which carries with it inherent risk factors as one of its basic characteristics related to resource sharing (multitenancy), such as regulatory, jurisdiction and privacy risks.

The observed papers are related to the AHP models for critical power systems:

Farzan et al. [54] propose a methodology for identifying critical substations and estimating cyber risks in the power grid. In the first phase of the proposed methodology, the most critical substation within the power grid is identified using the AHP and (*N-1*) simulation analysis to calculate the risk index for the substations within the power grid. The second phase of the methodology takes place at the substation level to identify its most critical components. This is followed by the repair (treatment) of the most critical vulnerabilities of electrical substation in order to optimize investment (cost) and reduce security risks, given the pervasive threats of cyber attacks by malicious hackers. Authors *Y. Ru et al.* also address the risk assessment of the power grid information system, but in the context of a possible cyber attack on the SCADA system itself [55]. In this case, the method for quantitative risk assessment is based on the attack tree model and the AHP. The following attributes were used to quantify the risk index in the AHP: loss of data packets, communication delay, harm to secondary equipment, impact on grid operations and economic losses. The disadvantage of this approach is that the interdependencies and feedbacks between these elements are not taken into account, but their relative independence is assumed.

In the following paragraph, the analyzed papers are grouped due to the use of Bayes' probability theory along with MCDM techniques in complex models for information security risk assessment purposes:

In a paper [56], a Bayesian prioritization procedure (BPP) for the AHP Group Decision Making support (AHP-GDM) is proposed to assess information security risks in case of incomplete information. MCDM techniques are mainly based on the assumption that complete data are provided on all model parameters (results, attribute weights), which is sometimes not possible in practice, so decision makers cannot express *n * (n - 1) / 2* possible judgments in reciprocal matrices of comparisons in pairs or express inconsistent judgments. It is Bayesian methods that make it possible to treat incomplete information using data augmentation techniques. In their work [57], Tan and Li also propose a group AHP decision-making model for the purpose of information systems risk assessment, which aims to determine the importance of risk factors where probability, impact and uncontrolability are defined as evaluation criteria and proposed alternatives are confidentiality attacks, integrity destruction, impersonation attacks, unauthorized access and denial of service. According to the defined risk criteria, the most significant security threats to the information system are evaluated through the group decision making process in order to reduce the subjective influence of personal preferences during the evaluation process itself. Wu and Zhao propose a generic privacy security risk assessment model for Internet of Things (IoT) based on Bayesian Networks (BN) and DEMATEL multicriteria decision-making technique [58]. In this model, the security analyst uses the BN to structure the risk propagation network and generate the likelihood of risk occurrence based on evidence inference. Thus, the decision makers can easily find the relevant propagation path that affects many asset risk factors. According to the conclusion in Bayesian networks, the probability of each propagation path can also be calculated. The DEMATEL technique is used to calculate influence weights for a propagation path that supports effective risk management decision making for IoT systems. It is actually a model for addressing the probabilistic causality of evaluation factors and gaining weights for influence-relation on propagation paths. The model assumes probabilistic inference and generates values for risk probabilities for assets and propagation paths using the Bayesian causal relational network and the previous probability. Although Bayesian statistics is not part of ISRA, the Bayesian approach is mentioned in the paper as an example of quality papers where its integration with some important MCDMs exists (e.g. AHP and particularly DEMATEL). This is very important because of network context and interdependencies of evaluation elements (i.e. information security risk attributes) that are envisioned to be part of the future research.

The following papers are related to the models created for dealing with information security incidents:

Anuar et al. [59] created their own Risk Index Model (RIM) to evaluate and rank IT security incidents using the AHP whereby the two main decision criteria were the likelihood of an event and its consequences, and each of these criteria had an additional 5 separate uncertain indicators, e.g. asset criticality, controls, impact severity, frequency, sensitivity. By combining elements and indicators for risk assessment together along with the AHP, the risk index for each indicator is quantitatively ranked. According to the results, the new risk model reduces the number of incidents and allows security analysts to focus solely on a smaller number of actual and critical incidents, which consequently reduces the time and resources. In an article [36], a new algorithm for ranking cyber security alerts for databases is proposed. The goal was to develop an AHP prioritization method that can automatically rank alerts at the level of risk posed by a particular transaction, thus allowing the security professionals to focus their time and efforts on the most important alerts. The proposed CyberRank model is a very important step in the direction of using some MCDM technique with security risk data samples to rank certain alternatives (in this case security alerts) when there is some uncertainty caused by lack of information, time and resources. Data samples and Python scripts used in this research are also available on the *GitHub* repository for the CyberRank model.

In the last paragraph of this papers' analysis, we present some other important works that were not being able to

categorize into some meaningful research stream due to the lack of more papers within the same stream:

Mohyeddin and Gharaee [1] demonstrated the application of a quantitative hybrid model obtained by modeling and synthesis methods to assess information security risk by combining FAHP and TOPSIS techniques, whereby such a new proposed hybrid model, according to the authors, yields more accurate results with a smaller error rate than the fuzzy AHP (FAHP). The aim was to create a new hybrid FAHP-TOPSIS model that minimizes the number of cross-comparisons that are necessarily made by using the AHP, in order to obtain greater accuracy in the estimates or a lower coefficient of variation than the standard FAHP. Therefore, a *t-test* of independent samples was performed to investigate the difference between the FAHP and the new proposed hybrid model, and the result was that the new proposed model had a smaller coefficient of variation, suggesting a lower error rate of the new model. Although the paper mentions the use of 3 levels of information security risk criteria in the evaluation, it does not specify exactly what the criteria are as well as their calculated weights. In their work [60], Moeti and Kalema identified the metrics required to design an information security management framework and classified them into categories, whereby metric validation was made by using the AHP. The results of the study indicate that environmental metrics are critical for managing information security, where in that category belong malicious code threats, inherent vulnerabilities in the information system and networks, and the regulatory and legal framework. However, it is surprising that the Risk Management category is ranked as the last of all the metric groups, which can certainly indicate an insufficient awareness of the importance of adequate information security risk assessment and management by examiners who have validated the proposed framework for measuring information security in an academic institution. To more accurately quantify asset threats and associated vulnerabilities, authors Su et al. in their paper [61] propose a methodology to conduct a risk assessment of computer network security by using the AHP and neural network. In doing so, the security risk analysis process is defined so that the identification of information assets is made through the identification of critical business processes, which is actually a crucial step because the assumption is that if the business process is secure then the information network is also analogous to that secure. Thereafter, activities continued to identify threats to information assets, then identify the vulnerabilities that each threat could exploit, calculate the risk for each asset, and finally calculate the systemic risk of the entire information network.

5.2 Discussion and recommendations

This section gives certain discussion and recommendations along with strengths and weaknesses derived from the results of the research.

A review of the literature revealed that in almost all analyzed studies some quantification was sought regarding the assessment and ranking of information security risks, risk factors or software solutions, and thus the use of some of the quantitative MCDM techniques was required. Such approach is appreciated and represents strengths of the research field because MCDM methods have strong mathematical foundations, and today the quantification of the level of risk to which information systems are exposed to (in terms of monetary values) is necessary in order to be able to measure it and help top management to take appropriate decisions. Also, it is clear from the research findings that there are various approaches and methods for ranking information security risks using some of the quantitative MCDM techniques, but also that in just a very few studies certain efforts have been made to integrate some basic ISRA elements or C-I-A attributes into the AHP, ANP, DEMATEL or TOPSIS techniques [39, 42, 44, 45]. We have noticed that the narrow field of risk assessment methods for the specific purpose of evaluation of IT solutions with MCDM application has not been explored sufficiently in scientific papers. This represents certain shortcomings of the research field, but also it's a very important roadmap and has an impact for the further research to extend the core ISRA elements, define their interdependencies, and integrate within one (or even more) of the MCDM techniques for the purpose to make a concrete evaluation of critical information systems in a more efficient and accurate way. Thus, there is a need for a new hybrid model for more effective and efficient evaluation of critical IT solutions by application of MCDM with the integration of elements for risk assessment. Such new model would be an important contribution to the field of information security, particularly risk domain.

Additionally, this literature research has revealed that there is a trend of developing hybrid models for risk analysis and assessment, and for deciding on the state of security or choosing an appropriate information system by using multicriteria decision-making (specifically indicated in the studies [38, 43]), which is actually a logical phenomenon of interdisciplinarity in conducting researches as information security risk management is necessarily integrated into other business domains, and thus becoming one of the top priority activities in protecting the assets and operations of each modern organization.

From this research, we discovered and analyzed that different MCDM methods are used in order to solve various problems in the field of information security risk management. So, in the following table, a short summarization is done:

Table 3. The recommended use of MCDM methods in the field of information security risk management

MCDM method	MCDM problem
AHP	Recommended for modest problems when there are no interrelated dependencies between evaluation criteria, e.g.: in cases when C-I-A security attributes are used as evaluation criteria; for ranking and evaluation of IT security incidents when only likelihood of an event and its consequences are defined as evaluation criteria; for ranking of cyber security alerts.
ANP and DEMATEL	Strongly recommended when risk evaluation criteria are mutually dependent and influence each other, and when necessary to create NRM (network relationship map) along the calculations of criteria weights.
TOPSIS	Suitable for solving BCM (Business Continuity Management) problems and ranking of critical and vulnerable information security controls when evaluation criteria are independent.
Delphi	Despite the *Delphi* is not actually a real MCDM method, but more a survey technique for collecting of anonymous opinions within the group of professionals, it's anyhow often used and recommended as an initial step before applying other MCDM methods. E.g., for structuring and defining key risk factors (criteria).

Table 3 gives an additional author's contribution based on the conducted SLR research to the field of information security risks by providing a systematization of the recommended application of MCDM methods.

6. CONCLUSIONS

Due to the significant increase of security threats and vulnerabilities, and very often the lack of time and resources to combat them efficiently in the business environment, prioritizing risks and addressing the most critical ones seems essential.

There are still many open issues in the field of information security risk assessment and risk management, and thus we believe that the application of MCDM in information security field is likely to remain popular with potential significant growth in the following years, particularly in creating new hybrid models.

This demanding systematic literature research analyzed the selected papers according to rigorous search criteria that seem the most prominent for the field of information security risk assessment with the application of multicriteria decision making. Thus, certain recommendations that could serve as a kind of best practices are provided for the use of MCDM in the information security risk field. It was discovered that, at the moment, there is no model for efficient evaluation of IT solutions. So, the future plan of the authors of this SLR paper is to conduct a new research in which the most important risk assessment elements could be identified by using *Delphi* technique in questioning relevant information security experts. Then, these elements would be integrated in some MCDM technique (or even more), and thus creating a new model for evaluation of critical IT solutions. Such model could be potentially more efficient for security evaluation and selection processes in comparisons to the current approaches used by organizations, and also would provide significant scientific contribution. The new model is planned to be created by using DSRM (Design Science Research Methodology) [101] approach.

REFERENCES

[1] Mohyeddin, M.A., Gharaee, H. (2014). FAHP-TOPSIS risks ranking models in ISMS. Proceedings of the 7th International Symposium on Telecommunications (IST), Tehran, Iran, pp. 879-881. https://doi.org/10.1109/ISTEL.2014.7000827

[2] Principles for the Sound Management of Operational Risk. Bank for International Settlements, June 2011.

[3] Von Roessing, R. (2010). An Introduction to the Business Model for Information Security. ISACA.

[4] ISO/IEC 27005:2018. Information technology – Security Techniques – Information Security Risk Management, Switzerland.

[5] ISO Guide 73:2009. Risk Management – Vocabulary.

[6] Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004.

[7] Guide for Conducting Risk Assessments. Information Security, NIST Special Publication 800-30, Revision 1, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, accessed on Jun. 21, 2018.

[8] ISO/IEC 27001:2013. Information Technology – Security Techniques – Information Security Management Systems – Requirements, Switzerland, 2013.

[9] Landoll, D.J. (2006). The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments. Auerbach Publications, Boca Raton, FL, US.

[10] Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Elsevier Inc., Waltham, MA, US.

[11] Kitchenham, B., Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. Keele University and Durham University Joint Report, EBSE Technical Report, UK.

[12] Inventory of risk assessment and risk management methods. ENISA ad hoc working group on risk assessment and risk management, European Network and Information Security Agency (ENISA), March 2006.

[13] Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, Technical Department of ENISA, Section Risk Management, European Network and Information Security Agency (ENISA), June 2006.

[14] Fenz, S., Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. IEEE Security & Privacy, 9(2): 58-65. https://doi.org/10.1109/MSP.2010.117

[15] Leszczyna, R., Egozcue, E. (2013). ENISA study: Challenges in securing industrial control systems. Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection, C. Laing, A. Badii and P. Vickers, Hershey PA: IGI Global. https://doi.org/10.4018/978-1-4666-2659-1

[16] Comparison of Risk Management Methods and Tools, ENISA, European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/comparison/comparison.html/, accessed on Jun. 23, 2018.

[17] Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security. https://www.cisa.gov/about-cisa/, accessed on Nov. 29, 2019.

[18] 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

[19] Pan, L., Tomlinson, A. (2016). A systematic review of information security risk assessment. International Journal of Safety and Security Engineering, 6(2): 270-281. https://doi.org/10.2495/SAFE-V6-N2-270-281

[20] Alcántara, M., Melgar, A. (2016). Risk management in information security: A systematic review. Journal of Advances in Information Technology, 7(1): 1-7. https://doi.org/10.12720/jait.7.1.1-7

[21] Chai, J., Liu, J.N.K., Ngai, E.W.T. (2013). Application of decision-making techniques in supplier selection: A systematic review of literature. Expert Systems with Applications, 40(10): 3872-3885. https://doi.org/10.1016/j.eswa.2012.12.040

[22] Paelinck, J.H.P. (1978). Qualiflex: A flexible multiple-

criteria method. Economics Letters, 1(3): 193-197. https://doi.org/10.1016/0165-1765(78)90023-X
[23] Edwards, W., Barron, F.H. (1994). SMARTS and SMARTER: Improved simple methods for multiattribute utility measurement. Organizational Behavior and Human Decision Processes, 60(3): 306-325. https://doi.org/10.1006/obhd.1994.1087
[24] Abdullah, L., Rabiatul Adawiyah, C.W. (2014). Simple additive weighting methods of multi criteria decision making and applications: A decade review. International Journal of Information Processing and Management, 5(1): 39-49.
[25] Saaty, T.L. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1): 83-98. https://doi.org/10.1504/IJSSci.2008.01759
[26] Saaty, T.L. (2001). Decision Making with Dependence and Feedback: The Analytic Network Process: The Organization and Prioritization of Complexity. RWS Publications, New York, US.
[27] Roy, B. (1991). The outranking approach and the foundations of electre methods. Theory and Decision, 31(1): 49-73. https://doi.org/10.1007/BF00134132
[28] Brans, J.P., Vincke, P. (1985). A preference ranking organisation method: The PROMETHEE method for multiple criteria decision-making. Management Science, 31(6): 647-656. https://doi.org/10.1287/mnsc.31.6.647
[29] Hwang, C.L., Yoon, K. (1981). Multiple Attribute Decision Making: Methods and Applications. Springer-Verlag, New York, US.
[30] Opricovic, S, Tzeng, G.H. (2004). The compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. European Journal of Operational Research, 156(2): 445-455. https://doi.org/10.1016/S0377-2217(03)00020-1
[31] Sumrit, D., Anuntavoranich, P. (2013). Using DEMATEL method to analyze the causal relations on technological innovation capability evaluation factors in Thai technology-based firms. International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 4(2): 81-103. https://tuengr.com/V04/081-103.pdf
[32] Hunjak, T. (1997). Mathematical foundations of the methods for multicriterial decision making. Mathematical Communications, 2(2): 161-169. https://hrcak.srce.hr/1808/, accessed on Aug. 16, 2018.
[33] Tzeng, G.H., Huang, J.J. (2011). Multiple Attribute Decision Making: Methods and Applications. CRC Press: A Chapman & Hall Book, Boca Raton, FL, US.
[34] Ishizaka, A., Nemery, P. (2013). Multi-criteria Decision Analysis: Methods and Software. Wiley, 1st Edition, UK.
[35] Stapić, Z., de-Marcos, L., Strahonja, V., Garcia-Cabot, A., Lopez, E.G. (2016). Scrutinizing systematic literature review process in software engineering. TEM Journal, 5(1): 104-116. https://dx.doi.org/10.18421/TEM51-16
[36] Grushka, H., Sofer, O., Biller, O., Shapira, B., Rokach, L. (2016). CyberRank: Knowledge elicitation for risk assessment of database security. ACM International Conference on Information and Knowledge Management (CIKM 2016), Indianapolis, Indiana, US, pp. 2009-2012. https://doi.org/10.1145/2983323.2983896
[37] Anikin, I., Emaletdinova, L.Y. (2015). Information Security Risk Management in Computer Networks Based on Fuzzy Logic and Cost/Benefit Ratio Estimation. International Conference on Security of Information and Networks, Sochi, Russia, pp. 8-11. https://doi.org/10.1145/2799979.2800022
[38] 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
[39] Yang, Y.P., 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
[40] Al-Safwani, N., Hassan, S., Katuk, N. (2014). A multiple attribute decision making for improving information security control assessment. International Journal of Computer Applications, 89(3): 19-24. https://doi.org/10.5120/15482-4222
[41] Al-Safwani, N., Fazea, Y., Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. Computers & Security, 77: 565-577. https://doi.org/10.1016/j.cose.2018.05.009
[42] Zhang, K., Shao, L. (2014). Research on the quantitative methods of classified information system security risk assessment. International Conference on Logistics, Informatics and Service Science (LISS), Beijing, China, pp. 571-575. https://doi.org/10.1007/978-3-662-43871-8_82
[43] Lee, M.C. (2014). Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. International Journal of Computer Science & Information Technology (IJCSIT), 1(1): 29-45. https://doi.org/10.5121/ijcsit.2014.6103
[44] Tianshui, W., Gang, Z. (2014). A new security and privacy risk assessment model for information system considering influence relation of risk elements. International Conference on Broadband and Wireless Computing, Communication and Applications (BECCA), Guangzhou, China, pp. 233-238. https://doi.org/10.1109/BWCCA.2014.76
[45] Hiete, M., Merz, M., Comes, T., Schultmann, F. (2012). Trapezoidal fuzzy DEMATEL method to analyze and correct for relations between variables in a composite indicator for disaster resilience. OR Spectrum, 34(4): 971-995. https://doi.org/10.1007/s00291-011-0269-9
[46] Kim, K.Y., Na, K.S. (2014). Business information system recovery priority decision using TOPSIS on interval data. Journal of Systems and Information Technology, 16(2): 103-112. https://doi.org/10.1108/JSIT-12-2013-0068
[47] Tsai, H.Y., Huang, Y.L. (2012). An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks. IEEE Transactions on Reliability, 60(4): 801-816. https://doi.org/10.1109/TR.2011.2170117
[48] Huang, Y.L., Sun, W.L. (2018). An AHP-based risk assessment for an industrial IoT cloud. IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, pp. 637-638. https://doi.org/10.1109/QRS-C.2018.00112
[49] Kim, H.J. (2012). Online social media networking and assessing its security risks. International Journal of Security and Its Applications, 6(3): 11-18.
[50] Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication

800-53, Revision 5, Appendix D, Joint Task Force Transformation Initiative, National Institute of Standards and Technology, April 2013. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft/, accessed on May 12, 2020.

[51] Zhu, R.X., Cui, X.J., Gong, S.J., Ren, H.K., Chen, K. (2014). Model for cloud computing security assessment based on AHP and FCE. International Conference on Computer Science & Education, Vancouver, BC, Canada, pp. 197-202. https://doi.org/10.1109/ICCSE.2014.6926454

[52] Fan, C.K., Chen, T.C. (2012). The risk management strategy of applying cloud computing. International Journal of Advanced Computer Science and Applications (IJACSA), 3(9): 18-27. https://doi.org/10.14569/IJACSA.2012.030903

[53] Alguliyev, R., Abdullayeva, F. (2014). Development of risk factor management method for federation of clouds. International Conference on Connected Vehicles and Expo (ICCVE), Vienna, Austria, pp. 24-29. https://doi.org/10.1109/ICCVE.2014.7297548

[54] Farzan, F., Jafari, M.A., Wei, D., Lu, Y. (2014). Cyber-related risk assessment and critical asset identification in power grids. IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, US, pp. 1-5. https://doi.org/10.1109/ISGT.2014.6816371

[55] Ru, Y., Wang, Y.F., Li, J., Yang, G.T., Yuan, K., Liu, K.P. (2016). Risk assessment of cyber attacks in ECPS based on attack tree and AHP. International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Changsha, China, pp. 465-470. https://doi.org/10.1109/FSKD.2016.7603218

[56] Eren-Dogu, Z.F., Celikoglu, C.C. (2012). Information security risk assessment: Bayesian prioritization for AHP group decision making. International Journal of Innovative Computing, Information and Control, 8(11): 8019-8032.

[57] Tan, Z., Li, P. (2012). Group decision-making information security risk assessment based on AHP and information entropy. Research Journal of Applied Sciences, Engineering and Technology, 4(15): 2361-2366.

[58] Wu, T., Zhao, G. (2014). A novel risk assessment model for privacy security in internet of things. Wuhan University Journal of Natural Sciences, 19(5): 398-404. https://doi.org/10.1007/s11859-014-1031-3

[59] Anuar, N.B., Papadaki, M., Furnell, S., Clarke, N. (2013). Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks, 6(9): 1087-1116. https://doi.org/10.1002/sec.673

[60] Moeti, M., Kalema, B.M. (2014). Analytical hierarchy process approach for the metrics of information security management framework. International Conference on Computational Intelligence, Communication Systems and Networks, Tetovo, Macedonia, pp. 89-94. https://doi.org/10.1109/CICSyN.2014.31

[61] Su, C., Li, Y.G., Mao, W., Hu, S.C. (2018). Information network risk assessment based on AHP and neural network. International Conference on Communication Software and Networks (ICCSN), Chengdu, China, pp. 227-231. https://doi.org/10.1109/ICCSN.2018.8488314

[62] Yu, Q., Shen, Y.J. (2016). Research of Information Security Risk Prediction based on Grey Theory and ANP. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, pp. 107-113. https://doi.org/10.1109/IMCEC.2016.7867182

[63] Meng, M. (2013). The research and application of the risk evaluation and management of information security based on AHP method and PDCA method. International Conference on Information Management, Innovation Management and Industrial Engineering, Xi'an, China, pp. 379-383. https://doi.org/10.1109/ICIII.2013.6703597

[64] Lai, Z., Shen, Y., Zhang, G. (2016). A security risk assessment method of website based on threat analysis combined with AHP and entropy weight. IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, pp. 481-484. https://doi.org/10.1109/ICSESS.2016.7883113

[65] Wu, X., Shen, Y.J., Zhang, G.D., Zhi, H. (2016). Information security risk assessment based on D-S Evidence theory and improved TOPSIS. IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, pp. 153-156. https://doi.org/10.1109/ICSESS.2016.7883037

[66] Samadi, H., Nazari-Shirkouhi, S., Keramati, A. (2014). Identifying and analyzing risks and responses for risk management in information technology outsourcing projects under fuzzy environment. International Journal of Information Technology & Decision Making, 13(6): 1283-1323. https://doi.org/10.1142/S021962201450076X

[67] Hosseini Bamakan, S., Dehghanimohammadabadi, M. (2015). A weighted monte Carlo simulation approach to risk assessment of information security management system. International Journal or Enterprise Information Systems, 11(4): 63-78.

[68] Grimaila, M.R., Badiru, A. (2013). A hybrid dynamic decision making methodology for defensive information technology contingency measure selection in the presence of cyber threats. Operational Research, 13(1): 67-88. https://doi.org/10.1007/s12351-010-0102-2

[69] Li, J. (2015). Mobile Advertising Security Risk Assessment Model Based on AHP. International Symposium on Computers and Informatics (ISCI), Beijing, China, pp. 1970-1978. https://doi.org/10.2991/isci-15.2015.259

[70] Zerkane, S., Espes, D., Le Parc, P., Cuppens, F. (2016). Vulnerability analysis of software defined networking. International Symposium on Foundations and Practice of Security (FPS), Quebec, Canada, pp. 97-116. https://doi.org/10.1007/978-3-319-51966-1_7

[71] Jiang, D.R., Liu, X.T., Li, Y.Y., Zhao, Y.W. (2016). The implementation and application of security evaluation system of electric power communication network. IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, pp. 1162-1165. https://doi.org/10.1109/CompComm.2016.7924887

[72] Yucel, G., Cebi, S., Hoege, B., Ozok, A.F. (2012). A fuzzy risk assessment model for hospital information system implementation. Expert Systems with Applications, 39(1): 1211-1218. https://doi.org/10.1016/j.eswa.2011.07.129

[73] Adetunji, O., Bischoff, J., Willy, C.J. (2018). Managing system obsolescence via multicriteria decision making.

Systems Engineering, 21(4): 307-321. https://doi.org/10.1002/sys.21436
[74] Peng, C., Shao, L. (2015). Classified information system security risk assessment model of the research. International Conference on Logistics, Informatics and Service Sciences (LISS), Barcelona, Spain. https://doi.org/10.1109/LISS.2015.7369664
[75] Geng, W., Hu, Y. (2012). Information security management model based on AHP. International Conference on Measurement, Information and Control (MIC), Harbin, China, pp. 352-355. https://doi.org/10.1109/MIC.2012.6273269
[76] Gao, H., Dai, Z.D., Peng, Y., Lu, H.K. (2014). Cyber security risk assessment of communication network of substation based on improved grey clustering. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, pp. 524-527. https://doi.org/10.1109/IIH-MSP.2014.136
[77] Wang, X., Jia, Y., Guo, L. (2016). Study on the function of computer technology in the electronic commerce environment security and risk assessment. International Conference on Intelligent Transportation, Big Data and Smart City, Halong Bay, Vietnam, pp. 784-786. https://doi.org/10.1109/ICITBS.2015.198
[78] Zhi, H., Zhang, G.D., Liu, Y.Q., Shen, Y.J. (2017). A novel risk assessment model on software system combining modified fuzzy entropy-weight and AHP. International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, pp. 451-454. https://doi.org/10.1109/ICSESS.2017.8342953
[79] Yudatama, U., Sarno, R. (2015). Evaluation maturity index and risk management for it governance using Fuzzy AHP and Fuzzy TOPSIS (case Study Bank XYZ). International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, pp. 323-327. https://doi.org/10.1109/ISITIA.2015.7220000
[80] Chen, L., Li, N.G., Chen, M., Li, Y., Xi, Z.S. (2018). Power mobile terminal security risk assessment based on AHP. International Conference on Smart Grid and Electrical Automation (ICSGEA), Changsha, China. https://doi.org/10.1109/ICSGEA.2018.00039
[81] Apriliana, A.F., Sarno, R., Effendi, Y.A. (2018). Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5. International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, pp. 373-378. https://doi.org/10.1109/ICOIACT.2018.8350708
[82] Wu, X., Li, X.H., Feng, R.T., Xu, G.Q., Hu, J., Feng, Z.Y. (2014). OOPN-SRAM: A novel method for software risk assessment. International Conference on Engineering of Complex Computer Systems, Tianjin, China, pp. 150-153. https://doi.org/10.1109/ICECCS.2014.28
[83] Ramalingam, D., Arun, S., Anbazhagan, N. (2018). A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM. International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2018), Gran Canaria, Spain, Procedia Computer Science, 134: 365-370. https://doi.org/10.1016/j.procs.2018.07.197
[84] Zhang, Y., Deng, X.Y., Wei, D.J., Deng, Y. (2012). Assessment of E-Commerce security using AHP and evidential reasoning. Expert Systems with Applications, 39(3): 3611-3623. https://doi.org/10.1016/j.eswa.2011.09.051
[85] Badie, N., Lashkari, A.H. (2012). A new evaluation criteria for effective security awareness in computer risk management based on AHP. Journal of Basic and Applied Scientific Research, 2(9): 9331-9347.
[86] Ntouskas, T., Polemi, N. (2012). STORM-RM: A collaborative and multicriteria risk management methodology. International Journal of Multicriteria Decision Making, 2(2): 159-177. https://doi.org/10.1504/IJMCDM.2012.046941
[87] Breier, J., Hudec, L. (2012). New approach in information system security evaluation. IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), Rome, Italy. https://doi.org/10.1109/ESTEL.2012.6400145
[88] Anikin, I. (2014). Information security risks assessment method based on AHP and fuzzy sets. International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM'2014), Istanbul, Turkey, pp. 6-10.
[89] Zheng, Y., Zheng, S. (2015). Cyber security risk assessment for industrial automation platform. International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Adelaide, SA, Australia, pp. 341-344. https://doi.org/10.1109/IIH-MSP.2015.58
[90] Cheng, Y. (2012). Information security risk assessment model of IT outsourcing managed service. International Conference on Management of e-Commerce and e-Government, Beijing, China, pp. 116-121. https://doi.org/10.1109/ICMeCG.2012.92
[91] Zhang, J., Zhao, J., Qian, X. (2012). Risk assessment of mobile payment system security based on extension theory. International Conference on Computer Science and Service System, Nanjing, China, pp. 880-883. https://doi.org/10.1109/CSSS.2012.224
[92] Hajrahimi, N., Hejazi Dehaghani, S.M., Sheikhtaheri, A. (2013). Health information security: A case study of three selected medical centers in Iran. Acta Informatica Medica, 21(1): 42-45. https://doi.org/10.5455/AIM.2012.21.42-45
[93] Drissi, S., Medromi, H. (2014). A new risk assessment approach for cloud consumer. Journal of Communication and Computer, 11(1): 52-58. https://doi.org/10.17265/1548-7709/2014.01007
[94] Ju, Y., Wang, A., You, T. (2015). Emergency alternative evaluation and selection based on ANP, DEMATEL, and TL-TOPSIS. Natural Hazards, 75(2): 347-379. https://doi.org/10.1007/s11069-014-1077-8
[95] Zaiyi, P. (2018). Network security situation analysis based on a dynamic Bayesian network and phase space reconstruction. The Journal of Supercomputing, 76: 1342-1357. https://doi.org/10.1007/s11227-018-2575-3
[96] Yan, C., Qiao, B. (2012). Study and application of risk evaluation on network security based on AHP. Communications and Information Processing (ICCIP 2012), Aveiro, Portugal, pp. 198-205. https://doi.org/10.1007/978-3-642-31968-6_24
[97] Librantz, A.F.H., dos Santos, F.C.R., Dias, C.G., da Cunha, A.C.A., Costa, I., de Mesquita Spinola, M. (2016). AHP modelling and sensitivity analysis for evaluating the criticality of software programs. APMS: IFIP International Conference on Advances in Production

Management Systems, Iguassu Falls, Brazil, pp. 248-255. https://doi.org/10.1007/978-3-319-51133-7_30

[98] Geng, F., Ruan, X. (2017). Campus network information security risk assessment based on FAHP and matter element model. Intelligent Computing Methodologies: International Conference on Intelligent Computing (ICIC 2017), Liverpool, UK, pp. 298-306. https://doi.org/10.1007/978-3-319-63315-2_26

[99] Comes, T., Mayag, B., Negre, E. (2014). Decision support for disaster risk management: Integrating vulnerabilities into early-warning systems. International Conference on Information Systems for Crisis Response and Management in Mediterranean Countries (ISCRAM-med 2014), Toulouse, France, pp. 178-191. https://doi.org/10.1007/978-3-319-11818-5_16

[100] Li, M., Bardi, M. (2014). A risk assessment method of cloud computing based on multi-level fuzzy comprehensive evaluation. International Conference on Cyberspace Technology (CCT 2014), Beijing, China. https://doi.org/10.1049/cp.2014.1377

[101] Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3): 45-78. https://doi.org/10.2753/MIS0742-1222240302