Technological and Economic Development of Economy

ISSN: 2029-4913 / eISSN: 2029-4921

2019 Volume 25 Issue 5: 979–997

https://doi.org/10.3846/tede.2019.10298

INFORMATION SECURITY MANAGEMENT FRAMEWORK SUITABILITY ESTIMATION FOR SMALL AND MEDIUM ENTERPRISE

Laima KAUŠPADIENĖ, Simona RAMANAUSKAITĖ*, Antanas ČENYS

Department of Information Systems, Vilnius Gediminas Technical University, Vilnius, Lithuania

Received 31 January 2019; accepted 12 April 2019

Abstract. Information security is one of the key concerns of an enterprise or organization. To assure suitable management of information security a list of information security management frameworks has been developed by a number of institutions and authors. A condensed information in information security management framework is very important to a small and medium enterprise as this type of enterprise usually lacks resources for information security expertise and deep analysis. Despite the fact, the information security management process and its frameworks, on the other hand, are very complex and require a big number of different elements. At the moment the comparison it is very shallow, as all properties of the comparison are treated equally important. In real life, the importance of different criteria of information security management framework and their suitability for small and medium enterprise vary. Therefore we use the Analytic Hierarchy Process to construct a hierarchy of information security management frameworks quality and applicability in small and medium enterprise and define the weights for each of the criteria. Weighted criteria express the importance of the criteria and executed the final comparison of alternatives (five information security management frameworks) is more realistic (similar to experts opinion) comparing to existing comparisons.

Keywords: information security management framework, suitability, small and medium enterprise, SME, multi-criteria, MCDM, AHP.

JEL Classification: C8, C63, M15, L53.

Introduction

Overarching digitalization is producing significant socio-cultural, economic and policy changes which create new opportunities, but also challenges and concerns for people and communities (Salminen & Hossain, 2018). The reliable and efficient infrastructure of an organization plays an important role, contributes to the preservation and strengthening of its financial stability and economic development. At the same time use of information and

*Corresponding author. E-mail: *simona.ramanauskaite@vgtu.lt*

communication technologies (ICT) concentrates various risks, associated with the formation of a modern living environment called cyberspace (Miloslavskaya &Tolstaya, 2017).

The risks of cybersecurity violation have acquired the status of systemic risks due to a significant increase in possible consequences from their implementation. The economics of information security decade ago become a thriving and fast-moving discipline (Anderson & Moore, 2006) and currently provides valuable insights not only for security experts but also for policymakers, business managers, economists and psychologists (Aminnezhad, Mahmod, & Abdullah, *et al*. 2016). Information security risk management is a top concern as information security incidents damage organization reputation, disrupt operations and are costly; information assets are more valuable and more vulnerable than ever; breaches and vulnerabilities have made information security the chief information officers' top priority (McLaughlin & Gogan, 2018). Nowadays cybersecurity is a major differentiator for organizations and an essential sustainable economic development factor (I. Vasiu & L. Vasiu, 2018). It is mandatory to develop the cybersecurity culture of ICT systems for users who have limited information about cybersecurity risks and cyber defence solutions (Udroiu & Vevera, 2018).

As states Safa, Von Solms, and Furnell (2015) "Technology cannot solely guarantee a secure environment for information; the human aspects of information security should be taken into consideration, besides the technical aspects". The importance of information security risk management to organizations development might be explained even by the fact the trust plays a significant role in shaping purchase intentions of a consumer (Oliveira, Alhinho, Rita, and Dhillon, 2017). Some groups of people (especially elder people) are a sceptic to ICT usage in their daily life. The scepticism increases with every new message in the media on client data leakage or other security attacks against the organization. Therefore the reputation on the internet is very important for e-commerce development and can be assured only by suitable information security management. Because of all these reasons, cybersecurity is one of the most notable organization risks concerns and information security management must be assured in every enterprise. However, there is evidence to suggest that security practices are not strongly upheld within small and medium enterprises as results of Lopes and Oliveira (2014) research reveal only 9% of SMEs has an organizational culture about information security. Mostly it is related to a lack of resources, therefore, despite the complexity of information security and its management, its assurance in a small and medium enterprise is even more challenging.

Despite the fact SME faces additional challenges comparing to big enterprises in the security management area, existing information security management frameworks are not fully adapted for SME usage. There are no clear criteria or methodology on how to evaluate the quality of the ISM framework, what are the most important criteria for ISM framework selection for a specific situation too. This is a very important problem for small and medium enterprise as they are lacking resources for information security assurance and at least clear guidelines could be provided in order to select a suitable ISM framework.

The *aim* of this research is to design a practical and reliable model for assessing information security management framework quality and suitability for application in SME.

In order to achieve the aim of the research, a list of ISM framework quality defining criteria have to be listed and weights for those criteria have to be assigned by using a suitable

multi-criteria decision-making model (MCDM). All this will be done in this research. The criteria and its weights will be applied for selected ISM framework and the results of this empirical analysis will be presented in this research too.

1. Related works

The comparison of information security management framework is important in order to select the most suitable for a specific situation or to measure its fullness, applicability etc. Therefore we analyze existing ISM frameworks and its comparison or quality measurement works.

1.1. Most known or recent information security management frameworks

At the moment there is no one superior information security management framework which would be able to cover all possible issues and would be easily implemented in the organization. Therefore currently there exist a large number of ISM frameworks, proposed by scientists, universally accepted organizations, business companies, governmental initiatives for protecting information security and others. All these ISM frameworks concentrate on a specific domain or have its own point of view.

Eloff and von Solms (2000) proposed a hierarchical framework for various approaches consisting of levels, where the top level of the hierarchical framework represents ICT in its broadest sense and includes all activities and all approaches adopted to ICT in general. This all-covering category is entitled Assessment of Information and Related Technologies. Despite the fact, the framework highlights the need to manage not only the hardware and software but ICT processes as well, an interconnection between different parts of the ISM is missing in it.

To solve this issue of stakeholder involvement, Trcek (2006) proposed an integral framework for information systems security management based on layered multi-panes. The author declares that in order to protect information, an organization has to start with the identification of threats related to business assets. Based on threats analysis, he proposed a layered multi-plane approach. The planes reveal different aspects in ISM but are oriented to information system security rather than enterprise security, therefore, does not ensure the overall security.

Bradley and Josang (2004) proposed an open framework for enterprise security management. This framework is intended to be a technology-dependent and comprises an information repository, manager programs, and configuration agents. At the same time since the proposed framework is technology-dependent, it will not provide the type of flexibility that may be required for SME.

Taking into account the needs of ISM in SME Sherwood, Clark and Lynas (2009) represented the SABSA (Sherwood Applied Business Security Architecture) framework for Enterprise Security Architecture. SABSA is intended for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. For easier applicability SABSA

a clear horizontal layer, where SME has to answer What (assets)? Why (motivation)? How (process and technology)? Who (people)? Where (location)? When (time)? SABSA is a generic architectural development framework that can be used for the operational-risk-based development and maintenance of operational capabilities in any type of business organization (SABSA Institute, 2019).

An organizational-level process model in Information security policy was proposed by Knapp, Morris, Marshall, and Byrd (2009) too. The model provides unique value through its comprehensive, real-world representation of an information security policy process in modern organizations. In the model, information security governance is an overarching category directly affecting the entire policy management process.

On 2017 Kauspadiene, Cenys, Goranin, Tjoa, and Ramanauskaite (2017) proposed a High-level self-sustaining information security management framework (HISMF). The framework was designed to adapt to the most important security standards and best practices. Distinguishing the ISM framework from others a wide list of stakeholders was added in order to present the wide area of information security assurance and different type stakeholders' incorporation into the enterprise operations. As well the ISM framework was adapted for usage in a small and medium enterprise – self-assessment sheet with associated information security maintenance, modelling and evaluation tools accompanied the framework.

This is the most known or recent ISM framework and the framework selection for a specific situation depends on many factors including industry sector and geography (E. Y. Kim & K. W. Kim, 2014).

1.2. Comparisons of information security management frameworks

The comparison of information security management or other related frameworks is mostly done to highlight specific factors, criteria of analyzed frameworks. This form is adapted in the commercial area too. For example, Health Information Trust Alliance [HITRUST] (2014) presents a brochure "Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53: Why Choosing the CSF is the Best Choice" where 12 factors are used to compare three analogues. The comparison is done in binary values by defining is the factor included in the analyzed framework or no. While the visual table-based presentation is well accepted the quality of analyzed frameworks is not reflected as factors might be unequally important, might have different complexity, granularity etc.

A similar system is used in most comparisons of information security area frameworks too:

- Rebollo, Mellado, Sánchez, and Fernández-Medina (2011) presented a comparative analysis of information security governance frameworks. The research aims to guarantee an objective comparison through a set of comparative criteria to highlight the strengths and weaknesses of each framework. Criteria for the comparison were selected from an analysis of existing information security governance papers, including both governance and management aspects. Meanwhile, the comparison is executed by defining the values of each criterion and no weights or importance factors are defined in the comparison.

- Alnuem, Alrumaih, and Al-Alshaikh (2015) executed a comparison study of information security risk management frameworks in cloud computing. The paper discussed how information security risk management is related to the cloud computing environment and presents seven different information security risk management frameworks that cover all of cloud service models and deployment models. Meanwhile, the comparison of mentioned frameworks was executed by summarizing framework information and classifying the frameworks according to the coverage area of the framework.
- Kauspadiene et al. (2017) together with the proposed high-level self-sustaining information security management framework executed a comparative analysis of other ISM frameworks. While other authors define evaluation criteria individually, in this research general and specific security objectives, presented by ENISA, grouped into five more abstract characteristics and used for ISM framework comparison. All analyzed frameworks were evaluated by the following defining characteristics: application of standards, implementation or performance model provided, whether the framework is a process or goal oriented, framework integration regarding different approaches and/or ISM levels. As well two more characteristics for the comparison of ISM frameworks were added by the authors: framework presentation in high-level abstraction concepts and different type of stakeholder presentation in the framework.

We were not able to find a source where information security management frameworks would be evaluated according to clearly defined and weighted factors. However, it is clear the comparison is a multi-criteria problem and should involve multi-criteria decision-making in order to select the best ISM framework.

1.3. Multi-criteria decision-making and its usage in the security area

Multi-criteria decision-making (MCDM) allows a decision-maker to choose the best alternative out of a number of alternatives or to arrange them based on multiple criteria (Hwang & Lin, 2012; Vinogradova, Podvezko, & Zavadskas, 2018). As multiple criteria exist, it is necessary to consider how each criterion influences the final decision, how to rank them or to estimate the weights for each of the criteria. In this field, multiple methods exist. Methods like ARAS (Zavadskas & Turskis, 2010), MULTIMOORA (Brauers & Zavadskas, 2010), MABAC (Pamučar & Ćirović, 2015), EDAS (Keshavarz Ghorabaee, Zavadskas, Olfat, & Turskis, 2015), are mostly dedicated for ranking alternatives, while AHP (Saaty, 1980), SWARA (Keršuliene, Zavadskas, & Turskis, 2010), R-SWARA (Zavadskas, Stević, Tanackov, & Prentkovskis, 2018) are mostly used for criteria weight definition.

While existing ISM framework comparison does not adopt the MCDM methods yet, the usage of MCDM is not new to information security area:

- Chemane et al. (2005) address the security mechanisms selection problem by proposing a multi-criteria decision-making model for structuring the VPN selection decision problem.
- Singh and Misra (2018) empirically investigate the critical challenges encountered by many firms for migration to cloud PLM. A multi-criteria decision-making method, grey Decision Making Trial and Evaluation Laboratory (DEMATEL) along with

interpretive structural modelling are employed to identify the causal challenges and their hierarchy to cloud PLM adoption. This empirical study brings out "data security" and "trust on solution provider" as the most important and critical challenges for migration to cloud PLM adoption.

- Dayanandan and Kalimuthu (2018) presented a software architectural quality assessment model for security analysis using fuzzy analytical hierarchy process (FAHP) method. The research results ensure that the proposed FAHP model with Buckley method performs better than existing methods in terms of security index to measure the performance at the SA level and defect density ratio to validate the results.
- Abdel-Basset, Manogaran, and Mohamed (2018) applied the internet of things in supply chain management by building a smart and secure system of supply chain management. For this, they presented DEMATEL and AHP in a neutrosophic environment to deal effectively with vague, uncertain and incomplete information.
- Bose, Biswas, Nandi, and Chakraborty (2018) presented a unified framework based on trust and multi-criteria decision-making for assuring security, reliability and QoS in DTN routing. The framework was called "Multi-Attribute Trust Evaluation and Management" (MATEM) and can be flexibly integrated with a large family of existing routing protocols to ensure secure, reliable and pervasive communication over a hostile DTN.
- Turskis, Goranin, Nurusheva, and Boranbayev (2019) solved the problem of ensuring the sustainable development of European Union countries in terms of identifying critical information infrastructures. Integrated multi-criteria decision-making techniques based on fuzzy WASPAS and AHP methods are used to identify essential information infrastructures, which are related to a new type of potential threat to national security.

This is just several examples of how multi-criteria decision-making models can serve in the field of information security. Comparing to other comparison methods the MCDM defines quantitative weights for each of multiple factors; therefore the quality measurement has a stronger justification. We believe the usage of MCDM models would benefit in the area of information security management framework quality and suitability for use in the small and medium enterprise too.

2. MCDM usage for ISM framework suitability estimation for usage in SME

As seen in the previous chapter, existing information security management frameworks might be very different. The variation exists because of different priorities and understanding of information security management in the organization. Therefore we want to define the most critical criteria and its importance for ISM framework suitability to be applied in small and medium enterprise and cover all needed security management areas.

2.1. Criteria and decision-making technique selection for ISM framework evaluation

From the linguistic analysis of the aim of this research, there can be noted two main evaluation areas: ISM framework applicability in small and medium enterprise and at the same time the ISM framework must serve as needed knowledge database for information security man-

agement. As these two criteria (applicability in SME and content of the ISM framework) are too abstract, they must be detailed. Therefore we selected the Analytical Hierarchy Process (AHP) methodology (Saaty, 1980) to be applied. AHP implements the hierarchical criteria structure which will be very handy in our situation. It is a multi-criteria decision-making technique and will represent the nature of multi-purpose security nature. AHP enables to combine a consensus of expert group by weighing the criteria and sub-criteria (Baudry, Macharis, & Vallée, 2018). The construction of the method is based on three steps: definition of the criteria structure; comparative evaluation of the substitutes and the criteria; synthesis of the priorities. AHP combines subjective assessments based on qualitative criteria and objective assessments based on quantitative criteria analytically (Saaty, Ozdemir, & Shang, 2015). According to Mardani et al. research results (Mardani, Jusoh, Zavadskas, Khalifah, & Nor, 2015), this is the most popular decision-making technique during the period from 2000 till 2014 in scientific papers as more than 30% of all 393 analyzed decision-making related papers were using this technique.

As mentioned above, we instinctively have the top level criteria: applicability in SME and content of the ISM framework. In order to leave no place for unfair second level criteria selection, we need a source which could serve as a reference model. In the case of criteria "content of the ISM framework" the most intuitive is the usage of security standard as a reference model. The most known and used information security management standard is ISO/IEC 27001 (International Organization for Standardization, 2013). This standard specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements of this standard may be certified by an accredited certification body following successful completion of an audit. The current version of this standard has 114 controls in 14 domains:

- A.5: Information security policies (2 controls).
- A.6: Organization of information security (7 controls).
- A.7: Human resource security (6 controls that are applied before, during, or after employment).
- A.8: Asset management (10 controls).
- A.9: Access control (14 controls).
- A.10: Cryptography (2 controls).
- A.11: Physical and environmental security (15 controls).
- A.12: Operations security (14 controls).
- A.13: Communications security (7 controls).
- A.14: System acquisition, development and maintenance (13 controls).
- A.15: Supplier relationships (5 controls).
- A.16: Information security incident management (7 controls).
- A.17: Information security aspects of business continuity management (4 controls).
- A.18: Compliance (with internal requirements, such as policies, and with external requirements, such as laws) (8 controls).

These fourteen control domains define the main areas of ISM framework content, therefore, we will use it a second level criterion as first level criteria "content of the ISM framework" sub-criteria (see Figure 1).

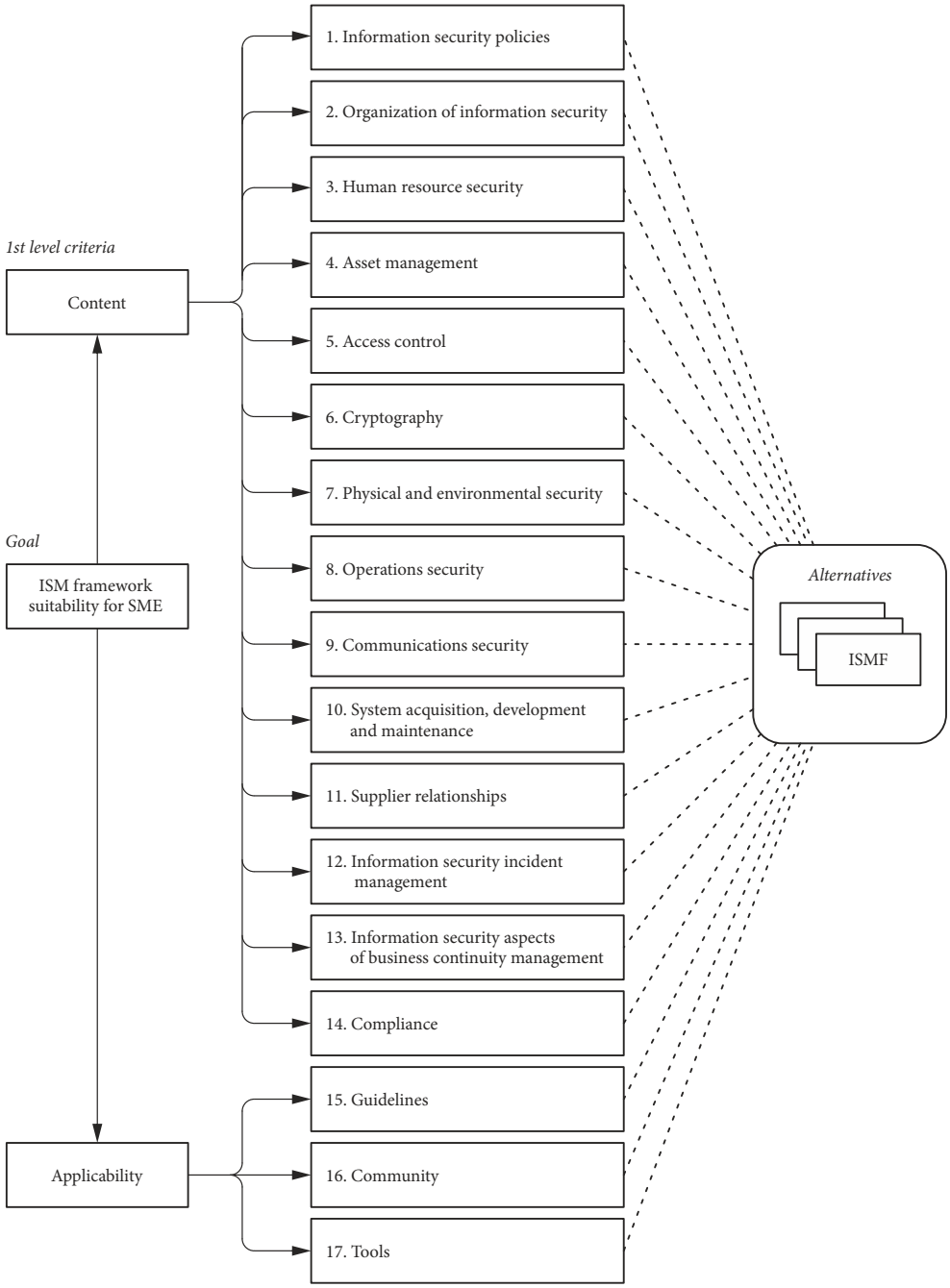

Figure 1. Proposed AHP structure for evaluation of information security management framework suitability for use in the small and medium enterprise

Criteria for "ISM framework applicability in the small and medium enterprise" does not have a clear reference model. There are no standards related to framework applicability in the small and medium enterprise. Meanwhile, the research papers are more concentrated on enterprise factors rather than the framework. For example the Eze, Olatunji, Chinedu-Eze, and Bello (2018) research "Key success factors influencing SME managers' information behaviour on emerging ICT (EICT) adoption decision-making in UK SMEs" derived sixteen key success factors influencing small business managers' information behaviour on emerging information and communication technologies. However, the factors defined the SME or its employee's properties rather than the properties of EICT. Therefore for the ISM framework applicability in the small and medium enterprise we proposed some second-level criteria by ourselves. It is very basic in order to be adaptable for a different type or purpose ISM frameworks and defines the ISM framework properties, influencing its easy integration into SME. The second level criteria are:

- Guidelines. In order to adapt the ISM framework, its content has to be understood correctly by the SME. Therefore the presentation of ISM framework has to be taken into account. Guidelines include clear documentation of the ISM framework. It might include some examples, visualizations or even training in order to help to understand and integrating the framework. It is important to all type of enterprise, however, it is very important to SME as it is lacking resources to analyze the ISM framework for a longer time, it must be as clear as possible from the first introduction to it.
- Community. Even if the ISM framework is fully acquired, some SME specific situations might be tricky and require additional consultations. Therefore it is important to have a community, which could help in discussion requiring situations. Big enterprises might buy additional training or consultations, meanwhile SMEs are lacking resources therefore publicly available and free of charge solutions are desired. The community might be defined by the popularity of the ISM framework as it leads to a bigger number of persons, able to share their experience. Forums or live help systems for the ISM framework information sharing might help and define the community possibilities.
- Tools. Information security management might be done by using human resources only, however, specified tools might simplify the information security management process. Therefore an ISM framework with dedicated or recommended tools leads to more modern information security management. The purpose of the ISM framework dedicated or recommended tools might vary from logging to modelling, situation evaluation or even decision support. SME would be able to adapt the tools and reduce the cost of manual information security management processes.

In total there are two first level criteria and seventeen-second level criteria in our applied Analytic Hierarchy Process. The criteria structure is presented in Figure 1. All criteria have descriptions in order to understand what should be taken into account in order to evaluate it.

The Analytic Hierarchy Process will be used for estimation of its weights and evaluating the information security management framework quality and suitability to be applied in the small and medium enterprise.

2.2. Criteria weights estimation and ISM framework comparison process

Criteria definition is important for alternative comparison, however in multi-criteria decision-making the importance, weight for each of the criteria has to be estimated. We use the standard methods of AHP technique: define the structure; evaluation the substitutes and criteria; synthesize the priorities. In order to eliminate the unconscious bias two groups of experts were used and the MCDM results were compared to ISM frameworks experts ranking (see Figure 2): as experts of ISM frameworks we prepare the hierarchy of criteria; external information security management experts evaluate the weights of the criteria; we rank the compared ISM frameworks according to our own believes for its suitability to be applied in SME; we estimate the values of second level criteria for each of compared ISM frameworks; the ISM framework ranking is compared to MCMD result for its validation.

In the criteria definition process, three information security management experts participated. These three ISM experts have at least 5 years of experience in information security management and currently, work in this area. Each ISM expert individually executed the pairwise comparisons of the same level sibling criteria. Traditionally AHP uses nine-point intensity of importance scale. We proposed an alternative solution to define the pairwise importance – dividing the 100% influence between two criteria. ISM expert is able to adjust the values interactively (see Figure 3) by assuming how the influence of those two criteria should be divided into percentages.

If the set of criteria are $C = \{ C_i \mid i = 1, 2, \ldots, n\}$, the results of the pairwise comparison of n criteria will be summarized in an evaluation matrix A of size $n \times n$. Every element a_{ij} (i, $j = 1, 2, \ldots, n$) in matrix A is the quotient of weights of the criteria (1).

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, \; a_{ii} = 1, \; a_{ji} = \frac{1}{a_{ij}}, \; a_{ij} \neq 1. \tag{1}$$

As ISM expert opinion is expressed as value from 0 to 100, we transform these values into evaluation matrix values. For transformation from 100% scale to AHP nine-point scale we use an Equation 2.

$$a_{ij} = \begin{cases} \dfrac{1}{Z\left(x_{ij}\right)}, \; x_{ij} < 50 \\ Z\left(50 - x_{ij}\right), \; x_{ij} \geq 50 \end{cases}, \tag{2}$$

there a_{ij} is a value of matrix A for criteria i and j; x_{ij} is ISM experts proposed influence value for criteria i comparing to criteria j; $Z(x)$ is a scale transformation function, presented in Equation 3.

$$Z\left(x\right) = 1 + \frac{8x}{50}. \tag{3}$$

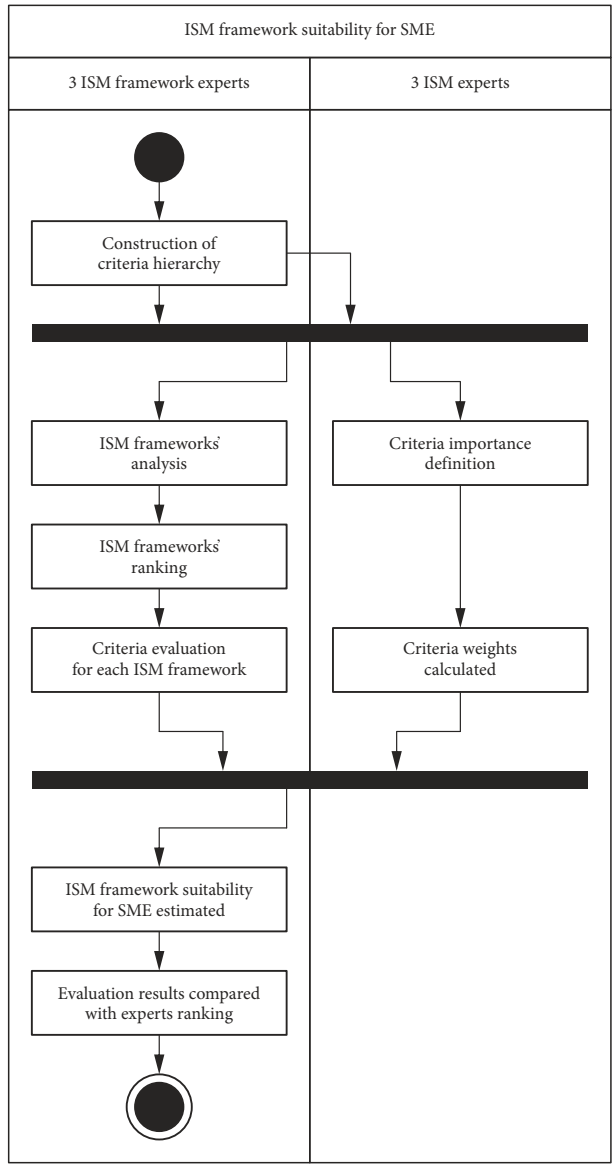

Figure 2. The process of the research: criteria hierarchy definition, criteria weight estimation, ISM framework ranking and evaluation according to defined criteria and their weights, MCDM result comparison to experts ranking

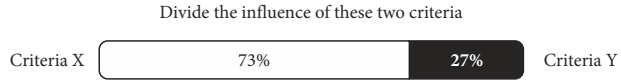

Figure 3. User interface example for executing the pairwise comparison by ISM experts

As we used three ISM experts opinion, the evaluation matrix *A* is formed based on the average value of these three ISM experts. The ISM experts were acting individually, however, their criteria importance marks in 100-scale were quite similar: the maximum difference between opinions of two ISM experts was 15%; standard deviation does not reach more than 9%. The average ISM experts mark was transformed into the nine-point system, the evaluation matrix was filled and Eigenvectors were calculated (see Table 1). For 1st level criteria, one weight is obtained, while for 2nd level criteria local weight is known as well as the global weight which is calculated as the product of 1st level and local weight.

Table 1. Criteria weights (Eigenvectors), calculated according to ISM experts pairwise evaluation

Criteria		Weight	
		Local	Global
ISM framework content		0.817	
	Information security policies	0.115	0.094
	Organization of information security	0.099	0.081
	Human resource security	0.126	0.103
	Asset management	0.054	0.044
	Access control	0.115	0.094
	Cryptography	0.023	0.019
	Physical and environmental security	0.043	0.035
	Operations security	0.095	0.078
	Communications security	0.071	0.058
	System acquisition, development and maintenance	0.051	0.042
	Supplier relationships	0.020	0.016
	Information security incident management	0.103	0.084
	Information security aspects of business continuity management	0.051	0.042
	Compliance	0.033	0.027
Applicability in SME		0.183	
	Guidelines	0.522	0.096
	Community	0.157	0.026
	Tools	0.321	0.059

Based on experts' opinion the ISM framework content is more important compared to its applicability in SME (the weight is 4.5 times greater for the first one). Meanwhile, if we would analyze the sub-criteria only, the second most important sub-criteria is guidelines (its global weight is 0.096) as part of applicability in SME criteria. This was influenced by the fact the guidelines are more important comparing to community and tools. However, the global weight of Human resource security (its global weight is 0.103), Information security policies (its global weight is 0.094) and Access control (its global weight is 0.094) is very close to the global weight of guidelines. These four sub-criteria have the biggest importance to ISM framework quality and applicability in SME and belong to the highest quartile of all

sub-criteria. All four sub-criteria are human-centered and highlight the need to take into account human nature while applying ISM frameworks in SME.

The second and third quartiles of sub-criteria global weights are mostly related to processes and their management. Meanwhile, the lowest quartile of sub-criteria global weights (Physical and environmental security – 0.035; Compliance – 0.027; Community – 0.026; Cryptography – 0.019; Supplier relationships – 0.016) is more related to technical, programmed solutions. The unimportance might indicate it is a must in any enterprise; however, in this experiment we do not analyze the reasons for weight distribution.

While the global weights are valuable for ISM framework comparison, the consistency confirmation is carried out to evaluate the degree of consistency between the pairwise comparisons. Results are presented in Table 2. Consistency ratio (CR) should not be calculated for top-level criteria as there are two sub-criteria only and the random index (RI) values are equal to 0. Meanwhile, CR values for ISM framework content and Applicability to SME sub-criteria are respectively 0.09 and 0.06. Consistency ratio value below 0.1 is a limit to threat the results as robust and we achieve a lower value as a prove for suitable pairwise comparison.

Table 2. Consistency evaluation metrics for criteria and sub-criteria

	Criteria	ISM framework content sub-criteria	Applicability in SME sub-criteria
Consistency index (CI)	0.00	0.14	0.03
Number of criteria (n)	2	14	3
Random index (RI) (Siraj et al., 2012)	0.00	1.57	0.52
Consistency ratio (CR)	–	0.09	0.06

The fact ISM experts' criteria pairwise comparison led to no intransitive judgments (three-way cycles) is also important. This fact shows the ISM experts have a clear understanding of the overall importance of all sibling criteria. The overall dissonance (Chen, Li & Wang, 2011) is more than 0 for ISM frameworks content sub-criteria as it has a big number of 2nd level criteria. However, the dissonance value is equal to 0.098 and does not require changes.

2.3. ISM frameworks' evaluation according to defined criteria and their weights

For ISM frameworks' evaluation, we selected 5 alternatives. These five frameworks were analyzed by three ISM framework experts and ranked from the best to the worst. All three ISM framework experts worked together and in discussion derived a consensus, one ranking. The analyzed ISM frameworks were ranked in this order:

1. Holistic information security management framework (Kauspadiene et al., 2017).
2. SABSA framework (Sherwook et al., 2009).
3. An organizational-level process model in Information security policy framework (Knapp et al., 2009).
4. Framework for information systems security management based on layered multi-panes (Trcek, 2006).
5. M. M. Eloff and S. H. von Solms hierarchical framework (Eloff & von Solms, 2000).

The ISM framework ranking was done in the beginning to make sure there is no preconception. The ISM framework evaluation criteria were defined after the ranking, so ISM framework experts used its own criteria to evaluate the ISM framework suitability for SME.

After the ISM framework evaluation criteria were defined, a list of criteria and their description was provided for the three ISM framework experts and they had to evaluate all five ISM frameworks according to all seventeen 2nd level criteria. For criteria evaluation, ISM framework experts were discussing and deriving a consensus mark. The mark had to be expressed in an interactive system (example provided in Figure 4), using linguistic values. The ISM framework expert opinions expressed in linguistic values are translated into the scale values exhibited in Table 3.

The results of the ISM framework evaluation are presented in Table 4. Both ISM framework experts proposed score values (score), as well as the values, multiplied by the weight of the criteria (weighted score), are presented and summed at the end of the table. According to the sum, the ranking was presented. The results prove the ranking according to the sum of not weighted scores do not meet the ranking of ISM framework experts opinion (the first and the second ISM framework had the same sum of not weighted scores, while the ranking was different by the ISM framework experts; the ranking of the third and the fourth ISM framework according to not weighted scores and ISM framework experts opinion are opposite). Meanwhile, the sum of weighted scores is well aligned with the ISM framework experts ranking.

Analysis of compared ISM framework suitability for small and medium enterprise showed none of the ISM frameworks fully meets the criteria. The maximum quality and applicability value is 71%. This means all of the frameworks have a place to improve.

The most important criterion for ISM framework quality and applicability in SME is Human resource security (global weight is 0.103), however only one framework was able to cover this area fully (score is 1.0, "excellent"), while the rest ISM frameworks take into account the human resource security from "none" to "good" out of what could be addressed in the framework. The second most important criteria (Guidelines) is not suitably implemented in existing ISM framework too as four ISM frameworks cover it just half as good as they could and only one has score 0.75, "good". This is a big issue as these criteria are the most important to SME and they do not have enough attention in most of the ISM frameworks.

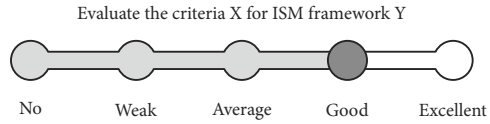

Figure 4. User interface example for executing the defined ISM framework criteria evaluation by ISM framework experts

Table 3. Linguistic values and scale values for ISM framework criteria meeting

Linguistic value:	no	weak	average	good	excellent
Scale value:	0.0	0.25	0.5	0.75	1.0

Table 4. Results of ISM framework suitability for usage in SME results

2nd level criteria	HISMF		SABSA		Knapp		Trcek		Eloff	
	Score	Weighted score	Score	Weighted score	Score	Weighted score	Score	Weighted score	Score	Weighted score
Information security policies	1.00	0.094	1.00	0.094	1.00	0.094	1.00	0.094	0.00	0.000
Organization of information security	1.00	0.081	0.50	0.040	1.00	0.081	0.75	0.061	0.50	0.040
Human resource security	1.00	0.103	0.75	0.077	0.50	0.051	0.50	0.051	0.00	0.000
Asset management	0.50	0.022	1.00	0.044	0.00	0.000	1.00	0.044	0.00	0.000
Access control	0.50	0.047	0.75	0.070	0.00	0.000	0.50	0.047	0.00	0.000
Cryptography	0.00	0.000	0.00	0.000	0.00	0.000	1.00	0.019	0.00	0.000
Physical and environmental security	0.50	0.018	1.00	0.035	0.50	0.018	1.00	0.035	0.00	0.000
Operations security	1.00	0.078	1.00	0.078	0.75	0.058	0.50	0.039	0.50	0.039
Communications security	1.00	0.058	1.00	0.058	0.50	0.029	0.00	0.000	0.00	0.000
System acquisition, development and maintenance	1.00	0.042	0.75	0.031	0.25	0.010	0.50	0.021	0.50	0.021
Supplier relationships	0.50	0.008	0.00	0.000	0.75	0.012	0.00	0.000	0.00	0.000
Information security incident management	0.00	0.000	0.00	0.000	0.50	0.042	0.00	0.000	0.00	0.000
Information security aspects of business continuity management	0.75	0.031	1.00	0.042	1.00	0.042	0.50	0.021	0.00	0.000
Compliance	0.75	0.020	0.75	0.020	0.75	0.020	0.50	0.013	1.00	0.027
Guidelines	0.50	0.048	0.75	0.072	0.50	0.048	0.50	0.048	0.50	0.048
Community	0.25	0.007	1.00	0.029	0.25	0.007	0.25	0.007	0.25	0.007
Tools	1.00	0.059	0.00	0.000	0.00	0.000	0.00	0.000	0.00	0.000
Sum:	11.25	0.716	11.25	0.690	8.25	0.512	8.50	0.500	3.25	0.182
Ranking:	1–2	1	1–2	2	4	3	3	4	5	5

Meanwhile, the criteria which are the best meat in all ISM frameworks are Information security policies (four frameworks fully cover the area and one framework do not give attention to it at all), Organization of information security, Operations security, Compliance (all five frameworks evaluated as average). These criteria are among the highest and lowest according to the global weight; therefore we were not able to find a pattern of how the score

relates to the global weight. Correlation between criteria global weights and ISM framework scores varies from –0.06 to 0.32 (HISM – 0.32; SABSA – 0.15; Knapp – 0.16; Trcek – 0; Ellof – (–0.06)) and shows none of the analyzed ISM frameworks was able to give the biggest attention to the most important criteria for SME. HISMF is the closest to mimic the criteria importance (mostly because of this he was ranked as first among others); however, has space to improve as well.

The experiment revealed the unique of some frameworks: Knapp proposed ISM framework is the only one, who covers (averagely, but takes into account) Information security incident management; HISMF is the only one with supplemented tools; Trcek ISM framework is unique as gives attention to cryptography.

Conclusions

In this paper, we overviewed several of the most known or recently published information security management frameworks, their comparison techniques and noticed there are no clearly defined criteria and their weights. This leads to a situation when no clear direction for ISM framework development is known and at the same time SME is not able to select the most suitable ISM framework without deep analysis and/or information security expert usage. This problem was solved in this paper by applying AHP and the following conclusions have been drawn:

1. Well-known security control domain usage (ISO/IEC 27001) as criteria list assures the consistency of pairwise comparison. Despite the fact there were fourteen criteria, no intransitive judgments (three-way cycles) were identified and the consistency ratio (CR) is less than 0.1.
2. Analyzed information security management frameworks are not optimized to fit the needs of the small and medium enterprise. The most suitable, with the biggest sum of weighted score information security management framework was able to reach 71% final score only. This was the only framework, which scores correlated to criteria weight (correlation coefficient was 0.32). This lead to a conclusion – information security management framework developers should concentrate on improvement of human-centred issues in order to be more adaptable by small and medium enterprises.
3. Defined information security management framework criteria and their weights are suitably assigned. Alternative ranking based on the sum of weighted scores were in 100% match with experts ranking, while the sum of non-weighted scores was not able to mimic experts ranking and led to three miss ranked positions for five alternatives. However, the calculated weights should be recalculated after some period of time, as the situation and understanding of information security management in the small and medium enterprise might change.

Author contributions

Laima Kaušpadienė and Antanas Čenys initiated the research. All authors together were responsible for design of analytical hierarchy process, ranking analyzed ISM frameworks and ISM framework evaluation according to 2nd level criteria. Laima Kaušpadienė executed the expertise of parwise criteria comparison (recruitment of the ISM experts, management of their work). Simona Ramanauskaitė prepared interactive tools for experts' opinion gathering. Laima Kaušpadienė and Antanas Čenys were responsible for data interpretation. Simona Ramanauskaitė wrote the first draft of the article.

References

Abdel-Basset, M., Manogaran, G., & Mohamed, M. (2018). Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Generation Computer Systems*, *86*, 614-628. https://doi.org/10.1016/j.future.2018.04.051

Alnuem, M., Alrumaih, H., & Al-Alshaikh, H. (2015). A comparison study of information security risk management frameworks in cloud computing. In *Cloud computing* (pp. 103-109). Retrieved from https://pdfs.semanticscholar.org/d495/a0732d0aaa211c05b1637975cbebb1009634.pdf

Aminnezhad, A., Mahmod, R., & Abdullah, M. T. (2016). Survey on economics of information security. *International Journal of Computer Science and Network Security (IJCSNS)*, *16*(7), 99-116.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613. https://doi.org/10.1126/science.1130992

Baudry, G., Macharis, C., & Vallée, T. (2018). Range-based Multi-Actor Multi-Criteria Analysis: A combined method of Multi-Actor Multi-Criteria Analysis and Monte Carlo simulation to support participatory decision making under uncertainty. *European Journal of Operational Research*, *264*(1), 257-269. https://doi.org/10.1016/j.ejor.2017.06.036

Bose, P. A., Biswas, S., Nandi, S., & Chakraborty, S. (2018). MATEM: A unified framework based on trust and MCDM for assuring security, reliability and QoS in DTN routing. *Journal of Network and Computer Applications*, *104*, 1-20. https://doi.org/10.1016/j.jnca.2017.12.005

Bradley, D., & Josang, A. (2004). Mesmerize: an open framework for enter-prise security management. In *Proceedings of the Second Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internation-Alisation* (Vol. 32, pp. 37-42). Australian Computer Society, Inc.

Brauers, W. K. M., & Zavadskas, E. K. (2010). Project management by MULTIMOORA as an instrument for transition economies. *Technological and Economic Development of Economy*, *16*(1), 5-24. https://doi.org/10.3846/tede.2010.01

Chemane, L. A., Ekenberg, L., Popov, O., Carrilho, S., Floor, R., & Mozambique, M. (2005). Government network and information security MCDM framework for the selection of security mechanisms. In *CNIS 2005*, 14–16 November, Phoenix, AZ, USA. Acta Press.

Chen, T., Li, Y., & Wang, H. (2011). A dissonance reduction method for intuitionistic fuzzy multicriteria decision-making problems. *Pan-Pacific Management Review*, *14*(1), 1-27.

Dayanandan, U., & Kalimuthu, V. (2018). Software architectural quality assessment model for security analysis using Fuzzy Analytical Hierarchy Process (FAHP) method. *3D Research*, *9*(3), 31. https://doi.org/10.1007/s13319-018-0183-x

Eloff, M. M., & von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. *Computers & Security*, *19*(3), 243-256. https://doi.org/10.1016/S0167-4048(00)88613-7

Eze, S. C., Olatunji, S., Chinedu-Eze, V. C., & Bello, A. O. (2018). Key success factors influencing SME managers' information behaviour on emerging ICT (EICT) adoption decision-making in UK SMEs. *The Bottom Line*, *31*(3/4), 250-275. https://doi.org/10.1108/BL-02-2018-0008

Health Information Trust Alliance. (2014). *Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53: Why Choosing the CSF is the Best Choice*. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/CSFComparisonWhitpaper.pdf

Hwang, C. L., & Lin, M. J. (2012). *Group decision making under multiple criteria: methods and applications* (Vol. 281). Springer Science & Business Media.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013. Information technology -- Security techniques -- Information security management systems -- Requirements*. Retrieved from https://www.iso.org/standard/54534.html

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (2017). High-level self-sustaining information security management framework. *Baltic Journal of Modern Computing*, *5*(1), 107. https://doi.org/10.22364/bjmc.2017.5.1.07

Keršuliene, V., Zavadskas, E. K., & Turskis, Z. (2010). Selection of rational dispute resolution method by applying new stepwise weight assessment ratio analysis (SWARA). *Journal of Business Economics and Management*, *11*(2), 243-258. https://doi.org/10.3846/jbem.2010.12

Keshavarz Ghorabaee, M., Zavadskas, E. K., Olfat, L., & Turskis, Z. (2015). Multicriteria inventory classification using a new method of evaluation based on distance from average solution (EDAS). *Informatica*, *26*(3), 435-451. https://doi.org/10.15388/Informatica.2015.57

Kim, E. Y., & Kim, K. W. (2014). A theoretical framework for cognitive and non-cognitive interventions for older adults: stimulation versus compensation. *Aging & Mental Health*, *18*(3), 304-315. https://doi.org/10.1080/13607863.2013.868404

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508. https://doi.org/10.1016/j.cose.2009.07.001

Lopes, I., & Oliveira, P. (2014). Understanding information security culture: a survey in small and medium sized enterprises. In *New Perspectives in Information Systems and Technologies* (Vol. 1, pp. 277-286). Cham: Springer. https://doi.org/10.1007/978-3-319-05951-8_27

Mardani, A., Jusoh, A., Zavadskas, E. K., Khalifah, Z., & Nor, K. M. (2015). Application of multiple-criteria decision-making techniques and approaches to evaluating of service quality: a systematic review of the literature. *Journal of Business Economics and Management*, *16*(5), 1034-1068. https://doi.org/10.3846/16111699.2015.1095233

McLaughlin, M. D., & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, *17*(3), 12.

Miloslavskaya, N., & Tolstaya, S. (2017). Organization's business continuity in cyberspace. In *First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures* (pp. 289-295). Cham: Springer. https://doi.org/10.1007/978-3-319-63940-6_41

Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior*, *71*, 153-164. https://doi.org/10.1016/j.chb.2017.01.050

Pamučar, D., & Ćirović, G. (2015). The selection of transport and handling resources in logistics centers using Multi-Attributive Border Approximation area Comparison (MABAC). *Expert Systems with Applications*, *42*(6), 3016-3028. https://doi.org/10.1016/j.eswa.2014.11.057

Rebollo, O., Mellado, D., Sánchez, L. E., & Fernández-Medina, E. (2011). Comparative analysis of information security governance frameworks: a public sector approach. In *The Proceedings of the11th European Conference on eGovernment–ECEG* (pp. 482-490). Academic Conferences Limited.

Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resources allocation*. New York, NY: McGraw.

Saaty, T. L., Ozdemir, M. S., & Shang, J. S. (2015). The rationality of punishment–measuring the severity of crimes: an AHP-based orders-of-magnitude approach. *International Journal of Information Technology & Decision Making*, *14*(01), 5-16. https://doi.org/10.1142/S0219622014500850

SABSA Institute. (2019). *Welcome to the official SABSA website*. Retrieved from http://www.sabsa.org

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record*, *54*(2), 108-118. https://doi.org/10.1017/S0032247418000268

Sherwood, J., Clark, A., & Lynas, D. (1995). *Enterprise security architecture* [white paper, 2009]. SABSA.

Singh, S., & Misra, S. C. (2018). Migration of PLM systems to cloud. *International Journal of Communication Systems*, *31*(18), 3815. https://doi.org/10.1002/dac.3815

Trcek, D. (2006). *Managing information systems security and privacy*. Springer Science & Business Media.

Turskis, Z., Goranin, N., Nurusheva, A., & Boranbayev, S. (2019). A fuzzy WASPAS-based approach to determine critical information infrastructures of EU sustainable development. *Sustainability*, *11*(2), 424. https://doi.org/10.3390/su11020424

Udroiu, A., & Vevera, V. (2018). Lifelong learning for raising cybersecurity awareness. In *12th International Technology, Education and Development Conference (INTED), 2018*. https://doi.org/10.21125/inted.2018.1272

Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. *European Journal of Sustainable Development*, *7*(4), 171-178. https://doi.org/10.14207/ejsd.2018.v7n4p171

Vinogradova, I., Podvezko, V., & Zavadskas, E. K. (2018). The recalculation of the weights of criteria in MCDM methods using the bayes approach. *Symmetry*, *10*(6), 205. https://doi.org/10.3390/sym10060205

Zavadskas, E. K., & Turskis, Z. (2010). A new additive ratio assessment (ARAS) method in multicriteria decision-making. *Technological and Economic Development of Economy*, *16*(2), 159-172. https://doi.org/10.3846/tede.2010.10

Zavadskas, E. K., Stević, Ž., Tanackov, I., & Prentkovskis, O. (2018). A novel multicriteria approach–rough step-wise weight assessment ratio analysis method (R-SWARA) and its application in logistics. *Studies in Informatics and Control*, *27*(1), 97-106. https://doi.org/10.24846/v27i1y201810