sciendo

DOI: 10.2478/orga-2022-0010

Outsource or not? An AHP Based Decision Model for Information Security Management

Luka JELOVČAN[1], Anže MIHELIČ[2], Kaja PRISLAN[2*]

[1]SGB, Varnostno svetovanje, d.o.o., Ljubljana, Slovenia

[2]University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia, *(corresponding author: kaja.prislan@um.si)

Purpose: Outsourcing information security has proven to be an efficient solution for information security management; however, it may not be the most suitable approach for every organization. This research aimed to develop a multi-criteria decision-making model that would enable organizations to determine which approach to information security management (outsourcing or internal management) is more suitable for their needs and capabilities.
Methods: Our study utilized several different research methods. First, the decision criteria were identified by reviewing related work and then selected by information security experts in a focus group. Second, a survey was conducted among information security practitioners to assign the criteria weights. Third, four use cases were conducted with four real-world organizations to assess the usability, ease of use, and usefulness of the developed model.
Results: We developed a ten-criteria model based on the analytic hierarchy process. The survey results promote performance-related criteria as more important than efficiency-focused criteria. Evidence from use cases proves that the decision model is useful and appropriate for various organizations.
Conclusion: To make informed decisions on approaching information security management, organizations must first conduct a thorough analysis of their capabilities and needs and investigate potential external contractors. In such a case, the proposed model can serve as a useful support tool in the decision-making process to obtain clear recommendations tailored to factual circumstances.

Keywords: *Information security, Decision model, Analytic hierarchy process, AHP, Management, Outsourcing*

1 Introduction

With the rise in the quantity and value of information, information security (IS) incidents and threat actors are also steadily increasing (Cisco, 2018). In 2019 alone, enterprises have reportedly suffered three and a half billion U.S. dollars in cybersecurity-related damages (Clement, 2020). As a result, the protection of information and information systems has become an important responsibility of modern organizations. While an IS program is necessary for organizations to survive, it requires substantial financial investments (Leszczyna & Litwin, 2020) and considerable managerial effort since information security management (ISM) is a complex task (Ponsard et al., 2018). Outsourcing has already been identified as a somewhat effective solution for efficient and cost-effective IS programs (Cezar et al., 2016).

However, outsourcing is not suitable for every organization, as it is also associated with various risks and uncertainties, such as hidden costs (Liu et al., 2018), loss of managerial control (Shahrasbi et al., 2017), and questionable quality of service (Feng & Chen, 2017). To determine whether outsourcing is an appropriate solution for their IS program, organizations must weigh between potential

Received: 3th November 2021; revised: 14th April 2022; accepted: 28th April 2022

risks and benefits of choosing such an approach. The emergence of potential risks varies based on the characteristics of individual organizations, their IS demands, and their financial and other resource capabilities (Beybutov, 2009). Organizations must thus consider many factors that vary in importance, which can be a demanding task. When approaching complex decisions, decision-makers often rely on decision models that serve as a tool for weighing different alternatives.

Decision models for information technology (IT) outsourcing have already been developed (e.g., Faisal & Raza, 2016; Pakpahan et al., 2021); however, a review of existing literature shows that no such model has been developed for deliberation over outsourcing and internal (in-house) ISM. Although there are a large amount of multi-criteria decision-making models (MCDM) available in the literature (Kabir et al., 2014), AHP is among the most appropriate MCDM methods for solving complex problems (Božičević et al., 2021; Ishizaka & Siraj, 2018). Hence, it was used by several researchers in IT management. Nonetheless, with a few exceptions (e.g., Faisal & Raza, 2016; Gulla & Gupta, 2011), most models only provide a theoretical AHP framework with identified but not prioritized decision criteria. Furthermore, use cases, which would support the usability of proposed models, are rarely provided. These shortcomings significantly lower the usability of existing decision models in practice and complicate the decision-making process for organizations. The main purpose of this paper is thus to present a scientifically based and practical decision model for ISM, designed for the decision-makers when optioning for the most appropriate ISM approach.

2 Preliminaries

2.1 Information security outsourcing

IS outsourcing can be an efficient solution for implementing and maintaining IS programs, specifically for organizations that do not possess the staff, funds, or knowledge to manage IS efficiently (Cezar et al., 2016). Outsourcing has already established itself as an efficient way to manage support services, such as accounting and sales (Popp et al., 2020), customer support call centers (Ren & Zhou, 2008), and legal services (Lacity & Willcocks, 2013). Since the "Kodak experiment" in 1989, IT has also become a popular outsourced support service (Dibbern et al., 2004).

Because of the growth and diversification of the IT field, IS soon became a service to be outsourced separately to maintain service quality (Fenn et al., 2002). In 2001, 19 percent of organizations reportedly outsourced their IT-related security services, while in 2018, a third of companies reported on such business practice (Cybersecurity Insiders, 2018). It is estimated that the managed security services providers (MSSP) market will keep growing, with a market value projection of 46.4 billion USD in 2025 (MarketsAndMarkets, 2020).

Organizations usually outsource a wide variety of IS services, from specific perimeter protection, including firewalls, intrusion detection systems, and virtual private networks, to more holistic security services, such as event monitoring and incident management (e.g., emergency response and forensic analysis) provided through SOCs. Despite the wide range of services that can be hired, a decision on whether to outsource or not and which IS service to outsource should be made upon considering the potential advantages, related risks, the needs of the organization, and its capability to perform the service internally (Wu et al., 2017).

There are several advantages of outsourcing IS. Most organizations mainly decide to outsource IS due to the cost-efficiency and more stable expenses (Sung & Kang, 2017). One crucial advantage of outsourcing is access to adequate resources, specialized technologies, advanced solutions, and a skilled workforce (Feng, Wang, et al., 2019). Moreover, MSSPs usually offer their services to several different enterprises, enabling them to detect IS risks quicker and more efficiently and distribute their knowledge across different organizations (Liu et al., 2018). Authors also note that mitigation of IS services enables management to focus more on their core activities (Ključnikov et al., 2019), perform faster incident response (Zúñiga & Jaatun, 2016), and improve regulatory compliance (Cezar et al., 2016).

Nevertheless, there are also disadvantages to IS outsourcing. Hiring an MSSP may not always result in predictable costs. It can lead to unplanned and hidden expenses since such relationships are influenced by the ever-changing cyberspace and threat landscape (Liu et al., 2018). Cutting costs can also lead to a decrease in service quality (Feng & Chen, 2017). One of the main risks of IS outsourcing is the loss of internal control over IS services (Shahrasbi et al., 2017). Outsourcing any kind of IT process generally presents a threat to IS, as it connects the organizational network with third-party information systems, which significantly expands the threat landscape (Feng, Wang, et al., 2019). For example, 53% of organizations reported a third-party information system-related security incident in 2019 (Ponemon Institute, 2019).

Other issues of IS outsourcing include issues related to the flexibility of the MSSP to provide their services across different and complex information systems (Beybutov, 2009). MSSP insider threats are also possible and a dilemma on what happens with the outsourced service if the MSSP goes out of business (Feng, Chen, et al., 2019).

Despite the many advantages of IS outsourcing, potential risks and issues can emerge if the process is not implemented properly. Since IS outsourcing is not appro-

priate for every organization, organizations must make an informed decision on how to manage the IS services. Decision models can provide a practical and efficient solution for such a dilemma, as they enable the organization to make rational decisions based on scientifically proven and validated decision factors.

2.2 Analytic hierarchy process

IS is a complex problem comprised of several security aspects (e.g., environmental security, device security, network monitoring, vulnerability scanning, virus prevention, data backup, access control, encryption, and intrusion detection (He & An, 2016). Hence there is a significant need for informed and comprehensive decision-making regarding its management. As already highlighted in the introduction, the AHP is a highly regarded MCDM method that has already been used in IT management research (Božičević et al., 2021; J. J. Wang et al., 2008). AHP divides complex problems into smaller pieces, making them more manageable. This helps decision-makers see those aspects isolated and independently to make more transparent and suitable decisions.

The AHP decision process is originally divided into three core phases (Saaty, 1990). However, to describe the AHP process in more detail, unequivocally, and comprehensively, we present this three-phase process in fourteen steps (Figure 1). In the first phase, a hierarchical structure for the decision model should be created (steps 1 – 4). In the second phase, relative priorities (local priorities) should be determined based on pairwise comparisons through a structured questionnaire (steps 5 – 9). The final phase is represented by a synthesis of the relative priorities into global priorities, which yields the final decision proposal (steps 10 – 14). Such compartmentalization of the process may be helpful for decision-makers to better differentiate between distinct phases and steps to be undertaken and understanding our model proposed in sections 3 and 4.

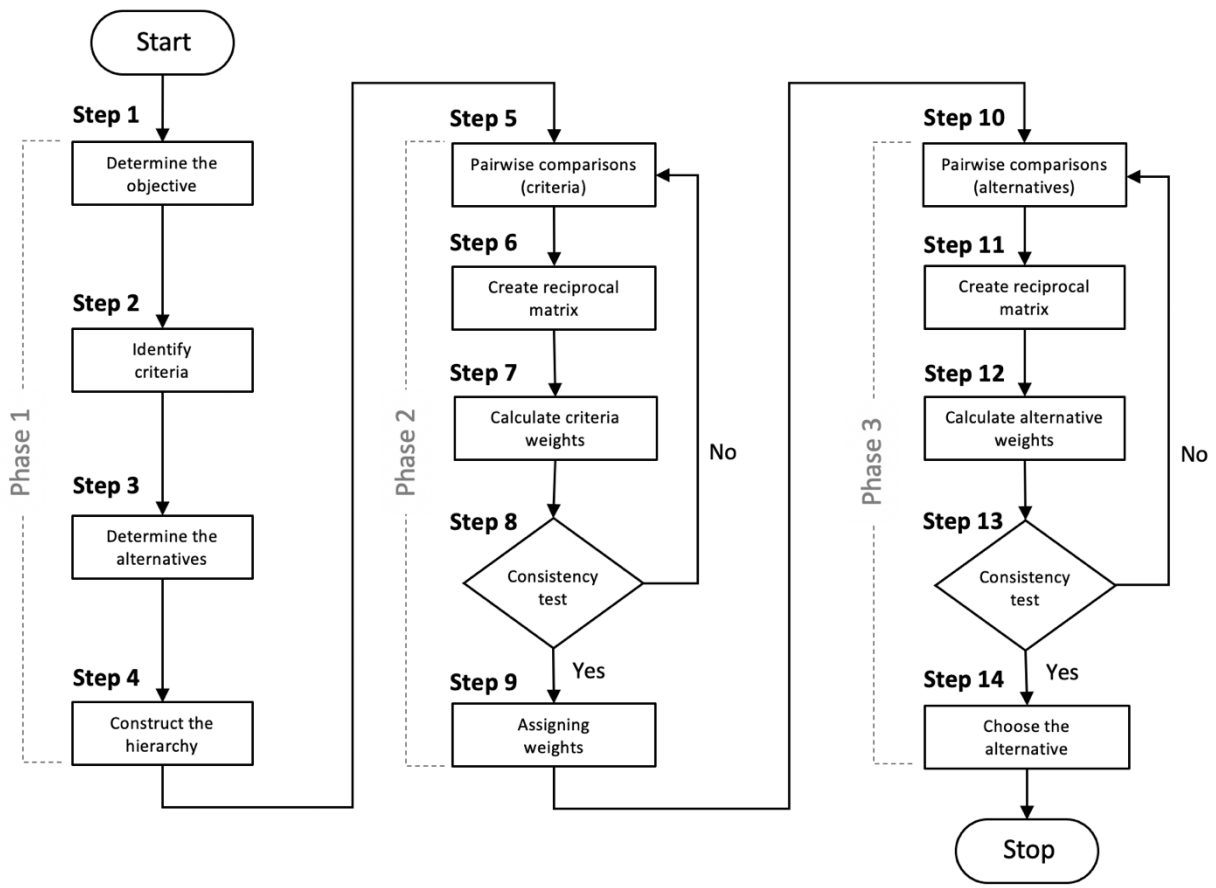


Figure 1: Analytic hierarchy process methodology overview

Phase 1. Step 1 (all steps in the following refer to Fig. 1) requires determining the main objective of the decision-making. In step 2, criteria influencing the decision-making process should be identified. Then at least two decision alternatives should be set in step 3, and a hierarchy model should be constructed in step 4. A picturesque example of an objective would be a decision on buying a house, where criteria for the decision could be location and year of construction, while alternatives would be a house A and a house B.

Phase 2. Step 5 is represented by the pairwise comparisons. Each identified criteria should be compared on a pairwise comparison scale in a structured questionnaire. The results enable determining the degree of preference for which criteria are more important and by how much. Even though a nine-point scale (with five principal values and four intermediate values) is recommended according to Saaty (1990), a lower number of scale points (e.g., scale without intermediate values) were also deemed sufficient and have been used in previous research (e.g., Harker and Vargas, 1987; G. Wang et al., 2009).

Following the previous example, a question may be: "Please choose which criterion when buying a house is more important to you and by how much." For example, criteria when buying a house might be location, price, and size. Criteria pairs are then compared, as seen in Figure 2.

Based on the results of pairwise comparisons, values are entered in a reciprocal comparison matrix in step 6. Values to the left of »1 – Equally important« are inserted above the diagonal of the matrix as absolute values, while values on the right side are inserted as reciprocal values. The part of the matrix below the diagonal is therefore filled with reciprocal values of the values above the diagonal so that j_ij= 1⁄j_ji . In case of the comparisons seen in Figure 2 (criteria Cri_x,Cri_y *and* Cri_z), the following reciprocal matrix is formed as follows:

$$A = \begin{bmatrix} 1 & \frac{1}{3} & 3 \\ 3 & 1 & 4 \\ \frac{1}{3} & \frac{1}{4} & 1 \end{bmatrix} \quad (1)$$

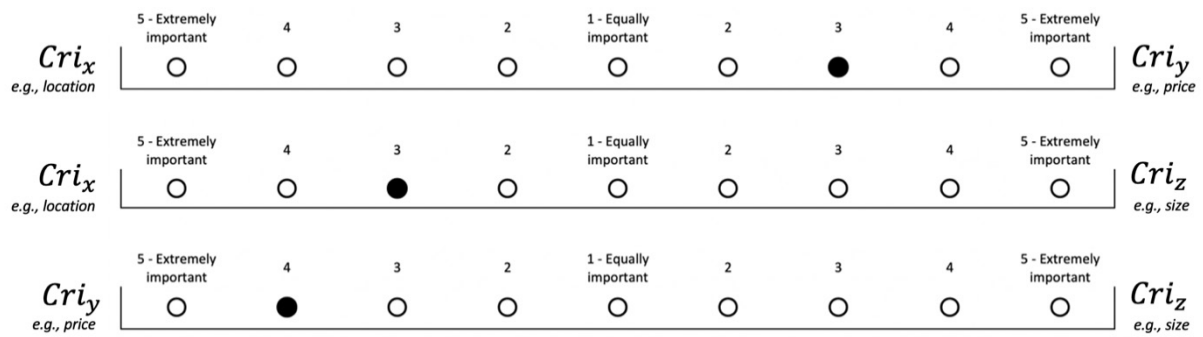


Figure 2: Example of pairwise comparison scale with selected preferences (Cri – criteria)

Weights are calculated from the reciprocal matrix with the eigenvalue method in step 7. Relative weights can be determined by the right principal eigenvector related to the largest eigenvalue of the reciprocal matrix *A*. Therefore, the vector of weights $\vec{w}$ satisfies the equation:

$$A \cdot \vec{w} = \lambda_{max} \cdot \vec{w} \quad (2)$$

where λ_{max} is the maximal eigenvalue. Relative weight w_i is calculated with the square root method:

$$w_i = \frac{\sqrt[n]{\prod_{j=1}^{n} j_{ij}}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} j_{ij}}} \quad (3)$$

When the relative weight is computed, λ_{max} can be determined:

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(Bw)_i}{w_i} \quad (4)$$

Since the evaluation requires a certain level of matrix consistency, the consistency test should be performed in step 8. The consistency index (*CI*) should be calculated as follows:

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (5)$$

where n is the number of independent rows in the matrix. If the matrix is perfectly consistent, then $CI=0$. However, the possibility of consistency error is increased with the increase of pairwise comparisons. Hence, the consistency ratio (*CR*) should be calculated as:

$$CR = \frac{CI}{RI} \quad (6)$$

where *RI* is a random index, represented by average *CI* values gathered from a randomly filled matrices. Usually, the *RI* is calculated based on 500 generated matrices (Ishizaka & Siraj, 2018). The *CR* value should range from 0 to 0.1. If the *CR* value exceeds 0.1, pairwise comparisons should be repeated. If the *CR* value is in the acceptable range, weights previously calculated according to (3) are assigned to all criteria (step 9).

Phase 3. Like pairwise comparisons of criteria in step 5, a pairwise comparison of the alternatives should also be conducted for each criterion in step 10. Following the previous example, a question may be: "Please choose which alternative is more important to you based on the location of the house – and for how much."

For creating a reciprocal matrix, calculating weights for alternatives and consistency ratio for comparisons (steps 11 – 12), steps 6 – 8 should be repeated. However, when only two alternatives are compared (e.g., outsourcing ISM and internal ISM), a consistency index will always equal CI=0. In such cases, step 13 can be omitted. Weight values assigned to the alternatives may range from 0 to 1, while their summation should always equal 1. The alternative with the higher weight value represents the proposed decision (step 14).

Calculations presented in this section are explained in more detail in Saaty (1980) and Markcikić & Radovanov (2011).

2.3 Related work

Since the decision on whether to outsource an IT service is a complex task, several decision models have been developed to help the management reach the right decision. Transaction cost theory, agency theory, and knowledge-based theory have been used frequently to determine which factors influence the decision to outsource IT-related services (Jain & Natarajan, 2011). These theories primarily focus on the cost-benefit perspective of outsourcing and promote factors such as strategic importance of service, outcome measurability and service observability, cost advantage, and service complexity. As such theoretical models explain the decision behind outsourcing, rather than provide the organization with help in the decision-making process, several more practice-oriented models have been developed. These are, in many cases, based on AHP.

Atkinson et al. (2015) developed an AHP decision model for IT services outsourcing based on factors such as financial, security, quality, technical, and relational risks. Similar risks have also been considered in other AHP-based decision models (Prakash et al., 2014). Factors associated with management, such as floating and scarcity of specialists, oversight over the service, and service flexibility, have also been identified as crucial for deciding on how to provide an IT service. Furthermore, the ability to focus on core competencies, which results in increased productivity, the strategic importance of the service, and flexibility to manage demand swings are business strategy-related factors that should also be considered (Khan et al., 2022). Other decision factors frequently considered in AHP-based decision models include technological factors, such as availability of state-of-the-art technology (J. J. Wang et al., 2008), economic factors, such as variability of expenses and levels of cost efficiency (Gulla & Gupta, 2011), and service quality (Fusiripong et al., 2020).

Even though several AHP decision models on IT security (e.g., risk modeling) and outsourcing IT services have been proposed in the literature (Gulla & Gupta, 2011; Faisal & Raza, 2016; Pakpahan et al., 2021; Prakash et al., 2014), to the best of our knowledge no IS outsourcing related AHP models had been developed. Other non-AHP-related studies, however, have already addressed several topics related to IS outsourcing. For example, the advantages and disadvantages of IS outsourcing have already been explored (Beybutov, 2009), as well as its risks (Liu et al., 2018). Wu et al. (2017) analyzed strategic decision-making and contractual relationships with MSSPs. Karyda et al. (2006) provided a strategic framework for choosing an IS outsourcing strategy, which includes several decision factors but can only be applied when an organization has already decided to outsource to address the security and privacy issues that may emerge outsourcing. Based on strategic hacker threats, Wu et al. (2020) focused on ensuring optimal levels of security services outsourcing.

Despite some established insights into IS outsourcing, no research has yet connected the findings of those studies to develop a decision model for deciding between internal and external management of IS services.

3 Research objectives and methodology

As ISM remains a problem for many organizations, an MCDM model that would utilize the findings of previous studies could help the decision-makers base their decisions on relevant factors related to the efficiency and quality of IS. To address the gaps in previous research, our main research objectives were to: 1) identify criteria crucial for efficient ISM, which form an essential base for decision-making on whether an IS services should be managed internally or outsourced; 2) prioritize the identified criteria; 3) develop an AHP based decision model for decision-makers in practice; and 4) assess the developed model for its usability, ease of use and usefulness.

To achieve the abovementioned objectives, we developed an AHP-based MCDM model for ISM by closely following the steps discussed in subsection 2.1 (see Figure 1). First, an objective of our model was set (step 1). Second, a structured review of related work was conducted to identify criteria that should be considered when deciding on the ISM approach. A focus group among IS experts was conducted to choose the ten most crucial criteria (step 2). Based on the literature review, the alternatives were determined, and the model hierarchy was proposed (steps 3—4). Next, a survey among IS practitioners was conducted to pairwise compare the identified criteria (step 5), followed by criteria prioritization and the consistency test using the AHP Online System software (Goepel, 2018) (steps 6—8). Finally, based on the results, weights were assigned to the individual criteria, and a final model was constructed (step 9).

At this stage, our model was developed and ready for use in organizations. To assess the model, we conducted four use cases in four organizations. Decision-makers in real-world organizations provided pairwise comparisons according to their needs and expectations (step 10). Based on the results, alternative weights were calculated and assigned to the alternatives (steps 11—13). In the follow-up survey, the proposed decision was communicated to the organizations (step 14) and discussed with their decision-makers or IT employees. An overview of the research methodology is presented in Figure 3.

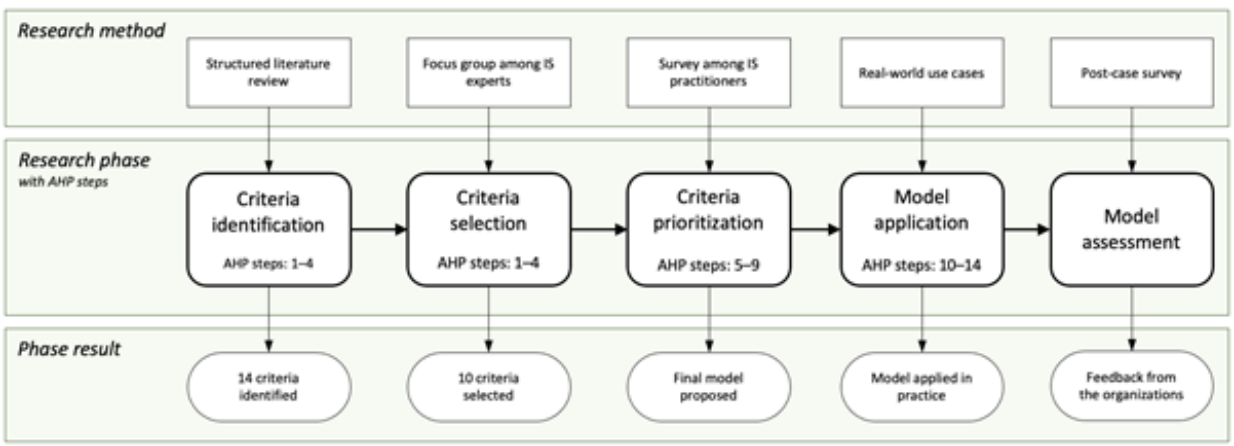


Figure 3: Overview of the research process matched with used methods and results in each phase

4 Model development

The primary objective of our AHP-based MCDM model is to provide organizations with the decision model for deliberating on how to approach ISM efficiently.

4.1 Criteria identification and selection

We identified factors (namely, criteria) contributing to such a decision-making process by reviewing related work on outsourcing. Since IS is strongly associated with IT management, the criteria that apply for ISM and IT management can be derived from existing AHP decision models for outsourcing IT services (J. J. Wang et al., 2008). When deliberating on an approach to IS services provision, criteria that are crucial to ensuring efficient and quality ISM should be the main deciding factors. To identify potentially relevant criteria, we reviewed and analyzed previous research on the discussed topics.

The review included research papers published since 2000. We focused on papers proposing decision models for outsourcing IT-related services and papers that included a description of criteria contributing to efficient ISM. The review revealed 14 unique decision criteria. We describe and summarize their relevance for efficient ISM in Table 1.

Table 1: Identified decision criteria

Criteria	Criteria description	Source
Threat awareness	The organization is well informed on current IS threats, vulnerabilities, and risks.	(e.g., Beybutov, 2009; Feng et al., 2019)
Knowledge of security solutions	The organization is well informed on the most prominent measures and solutions for efficient ISM.	(e.g., Feng et al., 2019; Wu et al., 2017)
Focus on core competence	The organization can maintain a high level of IS without affecting the quality of its core business processes. IS processes have minimal impact on other IT services inside the organization.	(e.g., Faisal & Raza, 2016; Ključnikov et al., 2019)
Flexibility	The organization can adapt its IS program to organizational changes, changes in its business processes, and changes in the threat landscape.	(e.g., Faisal & Raza, 2016; Rajaeian et al., 2015)
Regulatory compliance	The organization is familiar with key laws that regulate ISM, IT systems management, and personal data protection. All organizational activities related to IS follow the regulations.	(e.g., Beckers et al., 2013; Cezar et al., 2016)
Human resources	The organization has access to trained and experienced experts who specialize in executing and managing IS activities.	(e.g., Liu et al., 2018; Wu et al., 2017)
Tools and infrastructure	Adequate material resources (up-to-date software, hardware, and infrastructure) for quality ISM are available.	(e.g., Feng, Chen, et al., 2019; Ključnikov et al., 2019)
Moral hazard	There is a low risk that IT personnel will abuse their user and administrative privileges for malicious activity in the organization.	(e.g., Feng et al., 2019b; Liu et al., 2018)
Interdependency of security risks	The organization maintains a low risk of falling victim to an IS incident due to the connected information systems of business partners or other companies.	(e.g., Feng & Chen, 2017; Feng, Chen, et al., 2019)
Management oversight	The organization can actively control the processes connected to ISM.	(e.g., Aldya et al., 2019; Rajaeian et al., 2015)
Prompt response	The organization can detect IS incidents on time and can react promptly and appropriately.	(e.g., Sung & Kang, 2017; Feng et al., 2019b)
Organizations' reputation	Through quality ISM, the organization maintains the trust of its customers and business partners. The organization can demonstrate its security responsibility to keep the brand respected and recognized as trustworthy.	(e.g., Eduardovich & Vladimirovich, 2016; Zammani et al., 2019)
Business continuity	The organization has plans established for risk management and incident response. In case of an IS incident, the organization can ensure an undisturbed and continuous flow of business processes.	(e.g., Zammani et al., 2019; Chu & So, 2020)
Cost-efficiency	The approach to ISM is rational and economical, consistent with the organization's security and business needs and capabilities.	(e.g., Bojanc et al., 2012; Feng, Wang, et al., 2019)

Analysis of the related work extracted 14 criteria, which we reasonably deduced to ISM. While identified decision criteria individually cover different aspects of IS, it is also important to cover both the strategic and the operational view of managing IS services.

To optimize the process of pairwise comparisons, up to nine decision criteria are recommended on each hierarchical level in the analytic hierarchy process; however, it is not unusual to include ten or more criteria in AHP models (G. Wang et al., 2009). Since our literature review resulted in 14 criteria, we conducted a focus group to reduce the number of criteria to the most relevant ones, as suggested by (Russo & Camanho, 2015).

The ten focus group participants were experts in information and organizational security. Seven respondents were employed as researchers in information and organizational security, and three were employed in organizations providing security services. Their experience ranged from 4 to 20 years (M = 11.1 SD = 5.5). Participants had experience with research work and ISM and were thus able to make a balanced judgment on the importance of included criteria.

Focus group respondents were provided with a criteria description (see Table 1) and asked to evaluate their importance for efficient ISM. Each criterion was evaluated on a seven-point Likert-type scale. The phrase “criteria is completely irrelevant” was assigned to the value 1, and the phrase “criteria is extremely relevant” was assigned to the

value 7. In total, the questionnaire consisted of 14 items (criteria).

Table 2 presents the results of respondents' answers on the importance of individual factors.

We arranged the criteria based on their median values and discussed the results with the participants. The median value was chosen due to the relatively low sample size and use of an ordinal scale. The results show that business continuity, prompt response, cost-efficiency, knowledge of security solutions, and threat awareness most significantly contribute to efficient ISM. On the other hand, flexibility, the interdependency of security risks, moral hazards, and organizations' reputation are the least important for effective ISM and were thus eliminated from the further model development process. Higher standard deviations of the excluded criteria also suggest a higher level of disagreement among the respondents. Even though the median value of the criteria "tools and infrastructure" is relatively low, we concluded it should be included in the final decision model since it has been often highlighted as vital in previous research (Feng, Chen, et al., 2019; Liu et al., 2018). We finally included ten criteria in the decision model.

Table 2: Evaluation of criteria importance (Me – median, M – mean, SD – standard deviation)

Criteria	Me	M	SD
Business continuity	7.0	6.7	0.64
Prompt response	7.0	6.6	0.80
Cost-efficiency	6.5	6.1	0.94
Knowledge of security solutions	6.0	6.1	0.83
Threat awareness	6.0	6.0	0.77
Regulatory compliance	6.0	5.7	1.10
Focus on core competence	6.0	5.6	1.28
Management oversight	6.0	5.6	1.28
Human resources	5.5	5.6	0.66
Tools and infrastructure	5.5	5.4	1.02
Flexibility	5.5	5.4	0.92
Interdependency of security risks	5.0	5.3	1.19
Moral hazard	4.5	4.9	1.64
Organizations' reputation	4.5	4.9	1.45

Based on the identified criteria and a review of previous research, two alternatives for ISM were determined: (1) managing information security internally or (2) outsourcing information security services.

Next, the decision model was conceptualized by constructing the hierarchy. The first level of the decision model is represented by setting the objective – efficient approach to ISM in organizations. The second level is represented by the ten identified criteria. The two alternatives represent the third level. The model is presented in Figure 4 (standard AHP hierarchy visualization).

4.2 Criteria prioritization

In this research phase, we addressed the importance of individual criteria by conducting pairwise comparisons and allocating each criterion with a decision weight (prioritization).

We conducted an online survey among Slovenian IS practitioners to obtain the necessary data to calculate the weights. The questionnaire was designed for respondents to conduct pairwise comparisons of 10 selected criteria according to their importance for efficient ISM. Due to the time efficiency, reduced complexity, and ease of use (Moisaidis, 1999), a five-point pairwise comparison scale was used, with value 1 assigned to the phrase "criteria are equally important" and value 5 assigned to the phrase "criterion is significantly more important". Pairwise comparison questions were formatted in a way that two criteria were written on each side of the questionnaire, with values ranging from 5 to 1 to 5 written between both criteria (for example, see Figure 2). The respondents chose the number they felt best characterized which criterion was more important and by how much. The survey consisted of 45 pairwise comparisons and three demographic questions. We collected demographic data related to gender, years of professional experience with IT or IS, and position in the

organization held by the respondent.

We distributed the survey among IS practitioners who worked in the IS sector or as IS specialists in various organizations. These individuals are considered to have in-depth knowledge of IS-related activities and are thus able to determine the importance of each criterion for efficient ISM. We identified the respondents via LinkedIn, webpages of different organizations related to IS, webpages of various interest groups, and various professional publications. If the email address of the potential respondent was publicly available, the participation request was sent via email directly to the recipient. Otherwise, the participation request was sent via email to the organization where the potential respondent is employed. In addition to the invitation and link to the survey, an email included an attached document describing the criteria. The invitation was also distributed via the Chamber of Commerce and Industry of Slovenia and other IS-related organizations such as the ICT Technological Network of Slovenia and SRIP[1] Smart Cities and Communities. In total, we have directly contacted 37 individuals whose email addresses were publicly available, 29 organizations employing IS specialists, and four organizations that bring together IS specialists. We have received 31 responses from IS practitioners, out of which 25 were male, two were female, and four did not provide the answer. The average respondent has worked in IT or IS for 12.8 years; however, 43% of respondents worked in IT or IS for ten years or less. Six respondents were identified as CEOs, six as project managers, and three as CISOs, while others stated different specialized roles, such as consultant, system administrator, or SOC analyst.

To prioritize the criteria, we first calculated the modes of each comparison made by the IS practitioners in the previous step and created the reciprocal matrix. To ensure the highest accuracy of calculations, specialized software AHP Online System was used (Goepel, 2018). Additionally, the consistency ratio was calculated to ensure the validity of the results (Saaty, 1990). With the consistency ratio of 0.079, the calculated values meet the inconsistency requirements of AHP, which has to be lower than 0.1 (Saaty, 1990). The matrix with the calculated modes of each comparison, calculated weights (w), and standard deviations (SD) is presented in Table 3.

The weights explain to the decision-makers how important criteria are and how seriously they should be considered when deciding between internal management or outsourcing the IS service. Results indicate that prompt response, management oversight, and business continuity are the most important criteria for efficient ISM. On the other hand, threat awareness, human resources, and cost-efficiency appear to be the least important criteria for efficient ISM.

Based on the conceptual model, the model with corresponding weights for every criterion was constructed (Figure 4).

Table 3: Reciprocal matrix (w – criteria weights, SD – standard deviations)*

	1	2	3	4	5	6	7	8	9	10	*w*	SD
1	1	1.00	1.00	1.00	0.33	1.00	1.00	0.33	0.20	1.00	0.064	0.025
2	1.00	1	1.00	1.00	3.00	0.50	1.00	0.25	2.00	1.00	0.097	0.066
3	1.00	1.00	1	1.00	3.00	1.00	1.00	0.33	0.33	1.00	0.082	0.037
4	1.00	1.00	1.00	1	3.00	1.00	1.00	0.33	1.00	1.00	0.090	0.036
5	3.00	0.33	0.33	0.33	1	1.00	0.33	0.25	1.00	1.00	0.066	0.049
6	1.00	2.00	1.00	1.00	1.00	1	1.00	0.33	1.00	1.00	0.087	0.037
7	1.00	1.00	1.00	1.00	3.00	1.00	1	1.00	1.00	1.00	0.102	0.046
8	3.00	4.00	3.00	3.00	4.00	3.00	1.00	1	1.00	3.00	0.206	0.071
9	5.00	0.50	3.00	1.00	1.00	1.00	1.00	1.00	1	3.00	0.137	0.081
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.33	0.33	1	0.070	0.016

*Numbers from 1 to 10 in the first column and the first row represent individual criteria: 1 – Threat awareness, 2 – Knowledge of security solutions, 3 – Focus on core competence, 4 – Regulatory compliance, 5 – Human resources, 6 – Tools and infrastructure, 7 – Management oversight, 8 – Prompt response, 9 – Business continuity, and 10 – Cost-efficiency.

[1] Strategic Research & Innovation Partnership (slo. Strateško Razvojno Inovacijsko Partnerstvo)

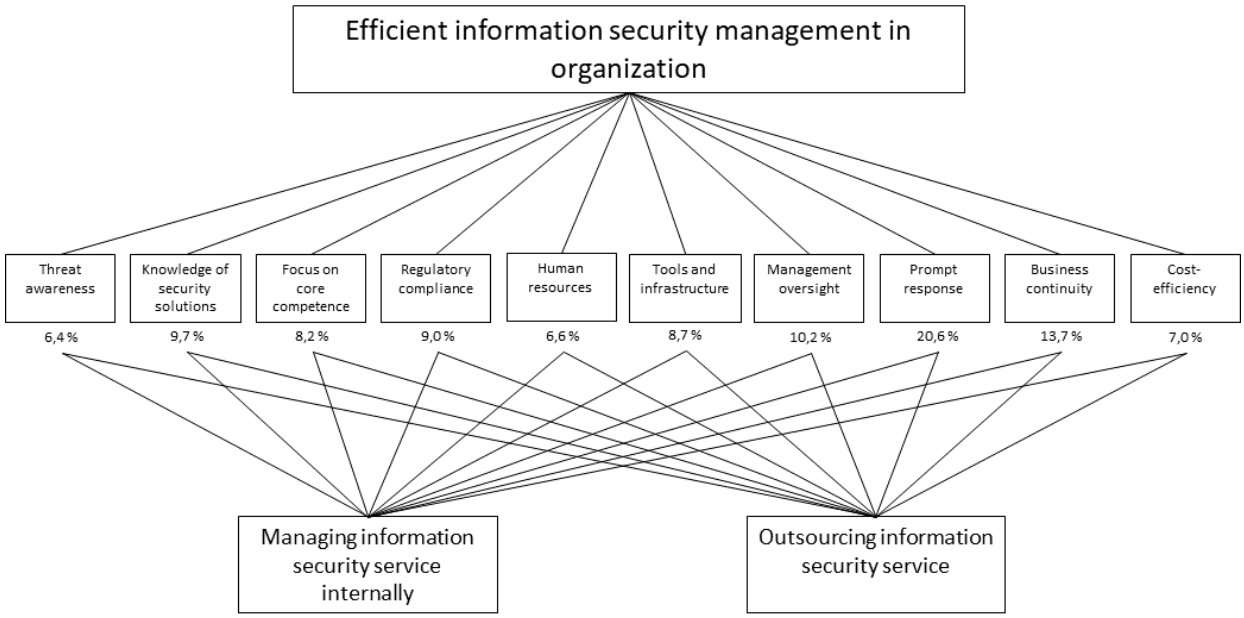


Figure 4: Developed decision model with assigned criteria weights

5 Model application

Thus far, the model development has been completed. Organizations that would like to use the model for deciding on the approach to ISM should now take steps 10 – 14. Since we compared only two alternatives, step 13 was omitted. To illustrate these steps and the use of the developed model, as well as to assess the model, we conducted four real-world use cases. Four organizations were selected by convenience sampling and included in the model assessment. Two organizations were sourced from the public sector, and two were sourced from the private sector. Organizations were invited to pairwise compare the two alternatives against all the criteria. To ensure the accuracy of calculations, we calculated alternative weights for the participating companies and communicated the results.

Each organization was asked to fill out an online survey where they compared the alternatives, considering each of the ten selected criteria (see Table 2) on a five-point pairwise comparison scale (for example, see Figure 2). Organizations were also asked to provide information on how dependent they are on IT, how high they rank the current state of IS in the organization, and how many employees are responsible for managing IT in the organization. Each organization was asked to forward the online survey to the employee(s) responsible for the IT management. Use cases are presented in the following subsections.

5.1 First use case

The first use case was conducted with a privately owned graphic design and retail company, employing between five and nine people (Spriv). The organization did not employ any staff dedicated to IT management. However, they were somewhat IT-dependent. Their self-reported level of IS in the organization was mediocre.

The results of the first use case are presented in Table 4. Results indicate that outsourcing IS is a preferred option. The organization preferred outsourcing concerning all criteria except for “focus on the core competence”.

5.2 Second use case

The second use case was conducted with a privately owned production and wholesale company, employing between 10 and 19 people (Mpriv). The organization had one employee dedicated to IT management and was highly dependent on IT. Their self-reported level of IS in the organization was mediocre.

Even though the results slightly turn towards in-house management of IS, the model does not decisively advocate any of the alternatives. The results of the second use case are presented in Table 5.

Table 4: Results of the first use case (w – criteria weights, W – alternative weight)

Criteria	*w*	Outsourcing	In-house
Threat awareness	0.064	3	0.33
Knowledge of security solutions	0.097	3	0.33
Focus on core competence	0.082	0.33	3
Regulatory compliance	0.09	3	0.33
Human resources	0.066	3	0.33
Tools and infrastructure	0.087	3	0.33
Management oversight	0.102	3	0.33
Prompt response	0.206	3	0.33
Business continuity	0.137	3	0.33
Cost-efficiency	0.07	3	0.33
W		**0.83**	**0.17**

Table 5: Results of the second use case (w – criteria weights, W – alternative weight)

Criteria	*w*	Outsourcing	In-house
Threat awareness	0.064	1	1
Knowledge of security solutions	0.097	2	0.5
Focus on core competence	0.082	2	0.5
Regulatory compliance	0.09	1	1
Human resources	0.066	0.5	2
Tools and infrastructure	0.087	3	0.33
Management oversight	0.102	0.2	5
Prompt response	0.206	1	1
Business continuity	0.137	1	1
Cost-efficiency	0.07	0.25	4
W		**0.49**	**0.51**

The organization deemed the alternatives evenly matched regarding four criteria and one alternative slightly more suitable concerning the remaining three criteria. Only in cases of management oversight and cost-efficiency in-house management of IS was identified to be significantly more suitable than outsourcing.

5.3 Third use case

The third use case was conducted with a publicly owned organization (primary school), employing between 10 and 19 people (Spub). The organization had one employee dedicated to IT management and was very dependent on IT. Their self-reported level of IS in the organization was mediocre.

Results indicate that in-house management of IS is the preferred option. The organization preferred in-house management concerning all criteria except for threat awareness and regulatory compliance. The results of the third use case are presented in Table 6.

5.4 Fourth use case

The fourth use case was conducted with a publicly owned organization (high school), employing between 100 and 149 people (Mpub). The organization had two

employees dedicated to IT management, and the organization stated that they are highly dependent on IT. Their self-reported level of IS was mediocre.

Even though the results slightly turn towards outsourcing IS, the model does not decisively advocate any of the alternatives. The results of the fourth use case are presented in Table 7.

Concerning the first six criteria, the organization did not distinguish between the alternatives. The organization did prefer outsourcing regarding the two most important criteria – prompt response and business continuity. The organization preferred in-house IS management regarding management oversight and cost-efficiency. However, since the organization mostly deemed all criteria equally important, the result does not significantly advocate one alternative as more suitable than the other.

Table 6: Results of the third use case (w – criteria weights, W – alternative weight)

Criteria	***w***	**Outsourcing**	**In-house**
Threat awareness	0.064	1	1
Knowledge of security solutions	0.097	0.2	5
Focus on core competence	0.082	0.2	5
Regulatory compliance	0.09	5	0.2
Human resources	0.066	0.2	5
Tools and infrastructure	0.087	0.2	5
Management oversight	0.102	0.2	5
Prompt response	0.206	0.2	5
Business continuity	0.137	0.2	5
Cost-efficiency	0.07	0.2	5
W		**0.15**	**0.85**

Table 7: Results of the fourth use case (w – criteria weights, W – alternative weight)

Criteria	***w***	**Outsourcing**	**In-house**
Threat awareness	0.064	1	1
Knowledge of security solutions	0.097	1	1
Focus on core competence	0.082	1	1
Regulatory compliance	0.09	1	1
Human resources	0.066	1	1
Tools and infrastructure	0.087	1	1
Management oversight	0.102	0.33	3
Prompt response	0.206	2	0.5
Business continuity	0.137	3	0.33
Cost-efficiency	0.07	0.33	3
W		**0.55**	**0.45**

6 Model assessment

In an additional follow-up survey, we provided the organizations included in use-cases with the results and asked them to provide feedback. In the form of four open-ended questions, the organizations were asked to state if they practice or would choose the same approach for ISM as the decision model suggested and to provide feedback on the perceived usefulness of the decision model for their organization and other organizations. Each organization was also asked to evaluate if the model is suitable for use in IS planning activities and the adequacy of the chosen decision criteria. At the end of the survey, respondents could freely discuss and comment on the decision model. The answers are presented in a consolidated form in the following.

Q1: Would you choose the same approach to ISM as suggested by the model?

All participating organizations agreed with the alternative suggested by the model and stated that they would choose the same approach as suggested by the decision model. Moreover, even though the result in the two cases was slightly ambiguous, the organization Mpriv highlighted that the result provided them a critical insight based on which they started considering outsourcing ISM and other IT-related activities, thus strengthening the level of their IS.

Q2: How suitable do you find the model for decision-making on ISM in your organization and/or other organizations?

All participating organizations stated that they find the developed model suitable for decision-making for ISM for their organization. Nonetheless, they agree that there might be some room for improvement. The improvement should primarily focus on tailoring the criteria to their specific organization. Pre-set criteria, however, provide a certain level of objectivity and reduce the stress of decision-makers in small organizations on whether chosen criteria are suitable for a particular ISM problem.

Q3: Would you choose this model for other information security-related decisions for your organization?

Participating organizations uniformly agreed on the model's suitability for any ISM problem. The reason predominantly lies behind pre-defined decision criteria, which ultimately play the same significant role in any IS-related decision-making. The organization Spub informally suggested pre-setting several AHP models based on these criteria addressing several major ISM problems. These pre-set models would be used in their future ISM decision-making.

Q4: How suitable do you find the criteria for ISM decision-making?

Participating organizations recognized the universal nature of the criteria used in the developed model. As previously mentioned, Spub suggested pre-setting several models that would address different ISM problems with the same criteria they find suitable and adequate. However, the organization Spriv would prefer a larger number of criteria based on which the alternative would be suggested, even though they find the current array of criteria adequate.

Participating organizations concluded that the approach to decision-making with the developed model is easy to use and does not require prior knowledge regarding AHP or other MCDM methods. Along with the fact that it is ready-made, it is a time-efficient method for decision-making for ISM. The results of the use cases suggest the model's usability, ease of use, and usefulness. Table 8 presents a summary of conducted use cases.

7 Discussion

Provision of IS is a vital function in mature organizations, as it contributes to their compliance, resilience, and social responsibility. However, IS is a complex system intertwined with many challenges related to organizational security needs, responsibilities, and capabilities. A thoughtful approach to the decision-making and management of such a system is thus necessary. Organizations can generally choose to manage IS internally or opt for outsourcing. However, the decision requires consideration of various factors as both approaches have several (dis) advantages. Consequently, many organizations face a dilemma on which approach is more appropriate.

The current study aimed to identify key criteria to consider in establishing efficient ISM and develop an MCDM model that helps organizations determine which approach to ISM is more suitable for their needs and capabilities. The results highlighted that business reputation and risks associated with the exertion of IS are among the least important criteria to be considered, albeit not insignificant. On the other hand, a prompt response is the most important criterion for an efficient ISM, which is consistent with the research findings of several previous studies. It is of utmost importance for fast incident detection (Zúñiga & Jaatun, 2016). It is also crucial in all steps of handling an incident, as it can contain the expansion of the breach and reduce the time in which business is limited due to the incident (Sung & Kang, 2017).

According to our research, business continuity and managerial oversight over IS activities are the two next most crucial criteria. Business continuity and IS are closely related, as each IS program must be designed to ensure business continuity (Chu & So, 2020). While business continuity is a consequence rather than an antecedent of the IS activities, our results suggest that the ISM approach needs to consider developing such capabilities and incorporate them into the planning stages. Furthermore, managerial oversight provides transparency and, to some effect, also looks after the legal aspects of the IS program (Georg, 2017). It can also provide a greater understanding of IS

Table 8: Summary of conducted use cases

ID.	Size (employees)	IT employees	IT dependency level	Current level of IS	Model result	Feedback summary
S_{priv}	5 – 9	0	Somewhat dependent	Mediocre	Outsourcing	The organization agrees with the model's result. They find the model and criteria suitable for them as well as for other organizations. Since they do not have any dedicated IT staff, the result was expected, but they still find the model interesting for possible future decisions on ISM.
M_{priv}	10 – 19	1	Completely dependent	Mediocre	In-house	The organization agrees with the model's result. They find the model valuable. The result encouraged them to incorporate security into their IT management process.
S_{pub}	10 – 19	1	Highly dependent	Mediocre	In-house	The organization agrees with the proposed approach. They find the model and criteria suitable for decision-making, and they will use the decision model in the future.
M_{pub}	100 – 149	2	Highly dependent	Mediocre	Outsourcing	The organization stated that they would choose the same approach as suggested by the model. They find the model and criteria suitable for them and other organizations. They also stated that the model is usable for further IS-related decision-making.

maturity and encourage appropriate financial and infrastructure support for the program (Atmojo et al., 2019).

The aforementioned criteria that were deemed most important focus on the IS performance rather than on the predispositions that need to be met for an efficient approach. Hence, organizations should primarily focus on the overall quality of service and consider costs, staffing, and technical aspects secondarily. While other studies suggest the importance of cost-efficiency (Wu et al., 2017), our results indicate that overall quality of service should be considered first if the primary goal is a mature and robust ISM. Certainly, costs and capabilities must not be overlooked in deciding on an ISM approach. However, increasing response time in exchange for lower costs should not be acceptable.

The results of four use cases performed in real-world organizations suggest that the proposed decision model is valuable and appropriate for various organizations. In the case of two organizations, the decision model strongly recommended in-house management and outsourcing, respectively, with both organizations agreeing with the proposal. In the case of two other organizations, the decision model did not decisively promote any alternatives. This occurs when the decision-maker using the model determines the alternatives as equally suitable regarding the criteria (Saaty & Tran, 2007). There are several potential reasons for such tentativeness. First, prior to using the model, organizations need to be aware of their abilities, needs, and resources. If the organization is not thoroughly familiar with its IS-related needs and resources, it can be hard to assess which alternative is more suitable regarding given criteria. Other studies addressing IT outsourcing also caution about the same issue (Feng, Chen, et al., 2019; Liu et al., 2018). Second, organizations can be indifferent toward certain factors (e.g., if the organization does not have the technical capabilities). In such a case, both alternatives can present a significant investment (Wu et al., 2017), leading to the organization not having a preference. Therefore, it is vital for organizations to thoroughly analyze their current state and capabilities of potential external contractors before comparing both options using the decision model. While the decision model only provided

explicit recommendations for two organizations, all four deemed the model as practical and helpful. Both organizations that were left without definite suggestions also indicated that the model raised their IS awareness, which further demonstrates its usefulness.

The use cases have also shown that scientifically supported systematic development of problem-solving methods does not necessarily provide clear solutions or answers. Solving real-world problems requires a thoughtful approach tailored to factual circumstances. Moreover, although complex problems are often solvable with straightforward solutions, we demonstrated that this is not always the case, especially in the circumstances related to high financial and security risks, such as IS in organizational settings. On this note, we can conclude that the proposed decision model is an effective tool and can be of great assistance in planning the organization's IS program; however, it should serve as a mere step in the decision-making process.

7.1 Implications, limitations, and future work

This research provides several theoretical and practical implications. To the best of our knowledge, this is not only the first AHP-based but also the first overall decision model explicitly developed for deliberating between outsourcing and in-house ISM. Our model is ready-made and to be used without having to identify and prioritize the decision criteria. This research also presents use cases where the developed decision model was utilized to emphasize its usability. Along with step-by-step guidelines provided in this paper, use cases provide a real-world assessment of the model and enable enterprises its straightforward application. Hence, the model can be directly applied to any small to a medium-sized organization aiming to plan an ISM. Use cases indicate that participating enterprises perceive the model as functional and easy to use. The developed decision model thus enables organizations a practical, scientifically substantiated, and systematic decision-making approach for ISM.

This research presents several limitations. First, since ten criteria were used to construct the decision model, some criteria had to be omitted. Even though scaling down the model was done to maintain the model's ease of use and overall usability (also suggested by Russo & Camanho (2015)), some of the omitted criteria could be considered important. Second, experts participating in the focus group and practitioners taking the survey were chosen by convenient sampling. Even though we provided different sizes of organizations and selected two organizations from the public sector and two from the private sector, convenient sampling was also used for choosing the participating enterprises. Third, pairwise comparisons were only made by IS specialists. Since we did not obtain the opinion of the managers, the model is slightly balanced toward the effectiveness of the IS and assigns less importance to the strategic criteria. Fourth, the model was not tested against any other decision model. Since such comparison was not possible due to the non-existence of similar decision models for ISM, we conducted a follow-up survey. The survey provided an alternative to such benchmark testing; however, further work on this topic is required.

Hence, our research findings and the developed model should serve as an incentive for further research. While our model provides adequate criteria weights for efficient decision-making, future work should provide a broader and more diverse sample of experts and practitioners to ensure higher uniformity in relevance assessments and prioritization of criteria. Likewise, decision-makers' opinions should be considered in the future to increase the validity of the decision model. Furthermore, future research should upgrade the model by including additional criteria across several hierarchical levels. That could also increase the model's validity and provide organizations with even more interpretable recommendations. In addition, the efficiency aspect must be more thoroughly investigated. Financial costs and investment in IS, for example, are well-researched topics (Bojanc et al., 2012); however, the costs and benefits of outsourcing are not investigated sufficiently.

Literature

Aldya, A. P., Sutikno, S., & Rosmansyah, Y. (2019). Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. *IOP Conference Series: Materials Science and Engineering*, *550*(1). https://doi.org/10.1088/1757-899X/550/1/012020

Atkinson, M. A., Bayazit, O., & Karpak, B. (2015). A case study using the Analytic Hierarchy Process for IT outsourcing decision making. *International Journal of Information Systems and Supply Chain Management*, *8*(1), 60–84. https://doi.org/10.4018/ijisscm.2015010104

Atmojo, T. A., Prabowo, H., So, I. G., & Abdinagoro, S. B. (2019). Improving information security performance: the role of management support and security operation center. *International Journal of Recent Technology and Engineering*, *8*(2), 4880–4886. https://doi.org/10.35940/ijrte.B3653.078219

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance. *Requirements Engineering*, *18*(4),

343–395. https://doi.org/10.1007/s00766-013-0174-7

Beybutov, E. (2009). Managing of information security with outsource service provider. In *International Siberian Conference on Control and Communications, SIBCON-2009,* (pp. 62–66). Tomsk, Russia: IEEE

Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing and Management*, *48*(6), 1031–1052. https://doi.org/10.1016/j.ipm.2012.01.001

Božičević, J., Lovrić, I., Bartulović, D., Steiner, S., Roso, V., & Škrinjar, J. P. (2021). Determining optimal dry port location for seaport Rijeka using AHP decision-making methodology. *Sustainability (Switzerland)*, *13*(11). https://doi.org/10.3390/su13116471

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2016). Sourcing Information Security Operations: The Role of Risk Interdependency and Competitive Externality in Outsourcing Decisions. *Production and Operations Management*, *26*(5), 860–879. https://doi.org/10.1111/ijlh.12426

Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability (Switzerland)*, *12*(8), 1–25. https://doi.org/10.3390/SU12083163

Cisco. (2018). *Annual Cybersecurity Report* (pp. 1-68). Retrieved from: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Clement, J. (2020). *Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2019.* Retrieved from: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

Cybersecurity Insiders. (2018). *Managed Security Report.* Retrieved from: https://www.cybersecurity-insiders.com/download-reports/

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information Systems Outsourcing: A Survey and Analysis of the Literature. *The Data Base for Advances in Information Systems*, *35*(4), 6–102. https://doi.org/10.1145/1035233.1035236

Eduardovich, D. V., & Vladimirovich, Y. A. (2016). Reputation risks through information security incidents. In *Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference, EIConRusNW 2016,* (pp. 194–198). St. Petersburg, Russia; St. Petersburg Electrotechnical University.

Faisal, M. N., & Raza, S. A. (2016). IT outsourcing intent in academic institutions in GCC countries: An empirical investigation and multi-criteria decision model for vendor selection. *Journal of Enterprise Information Management*, *29*(3), 432–453. https://doi.org/10.1108/JEIM-05-2015-0042

Feng, N., & Chen, B. (2017). An Integrated Strategy for Information Security: Outsourcing and In-house. In E. Qi, J. Shen & R. Dou (Eds.), *Proceedings of the 23rd International Conference on Industrial Engineering and Engineering Management 2016,* (pp. 305–309). Bali, Indonesia: Atlantic Press.

Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2019). To outsource or not: The impact of information leakage risk on information security strategy. *Information and Management*, *57*(5). https://doi.org/10.1016/j.im.2019.103215

Feng, N., Wang, M., Li, M., & Li, D. (2019b). Effect of security investment strategy on the business value of managed security service providers. *Electronic Commerce Research and Applications*, *35*(March), 100843. https://doi.org/10.1016/j.elerap.2019.100843

Fenn, C., Shooter, R., & Allan, K. (2002). IT security outsourcing: How safe is your IT security? *Computer Law and Security Report*, *18*(2), 109–111. https://doi.org/10.1016/S0267-3649(02)03009-1

Fusiripong, P., Baharom, F., & Yusof, Y. (2020). Analytic hierarchy process with firefly algorithm for supplier selection in IT project outsourcing. *Journal of Theoretical and Applied Information Technology*, *98*(8), 1255–1269.

Georg, L. (2017). Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management and Governance*, *21*(4), 793–814. https://doi.org/10.1007/s10997-016-9358-0

Goepel, K. D. (2018). Implementation of an Online Software Tool for the Analytic Hierarchy Process (AHP-OS). *Journal of the Analytic Hierarchy Process*, *10*(3), 469–487. https://doi.org/10.13033/ijahp.v10i3.590

Gulla, U., & Gupta, M. P. (2011). Deciding the level of information systems outsourcing: Proposing a framework and validation with three Indian banks. *Journal of Enterprise Information Management*, *25*(1), 28–59. https://doi.org/10.1108/17410391211192152

Harker, P. T., & Vargas, L. G. (1987). Theory of Ratio Scale Estimation: Saaty's Analytic Hierarchy Process. *Management Science*, *33*(1), 1383–1403. https://doi.org/10.1287/mnsc.33.11.1383

He, M. X., & An, X. (2016). Information security risk assessment based on analytic hierarchy process. *Indonesian Journal of Electrical Engineering and Computer Science*, *1*(3), 656–664. https://doi.org/10.11591/ijeecs.v1.i3.pp656-664

Ishizaka, A., & Siraj, S. (2018). Are multi-criteria decision-making tools useful? An experimental comparative study of three methods. *European Journal of Operational Research*, *264*(2), 462–471. https://doi.org/10.1016/j.ejor.2017.05.041

Jain, R. K., & Natarajan, R. (2011). Factors influencing the outsourcing decisions: A study of the banking sector in India. *Strategic Outsourcing: An In-*

ternational Journal, *4*(3), 294–322. https://doi.org/10.1108/17538291111185485

Kabir, G., Sadiq, R., & Tesfamariam, S. (2014). A review of multi-criteria decision-making methods for infrastructure management. *Structure and Infrastructure Engineering, 10*(9), 1176-1210. https://doi.org/10.1080/15732479.2013.795978

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, *14*(5), 403–416. https://doi.org/10.1108/09685220610707421

Khan, G. M., Khan, S. U., Khan, H. U., & Ilyas, M. (2022). Challenges and practices identification in complex outsourcing relationships: A systematic literature review. *PLoS ONE*, *17*(January). https://doi.org/10.1371/journal.pone.0262710

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues*, *6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Lacity, M. C., & Willcocks, L. P. (2013). Legal process outsourcing: the provider landscape. *Strategic Outsourcing: An International Journal*, *6*(2), 167–183. https://doi.org/10.1108/SO-11-2012-0021

Leszczyna, R., & Litwin, A. (2020). Estimating the Cost of Cybersecurity Activities with CAsPeA: A Case Study and Comparative Analysis. In S. Kanhere, In T. Patil, S. Sural, & M. S. Gaur (Eds.), *16th International Conference on Information Systems Security, ICISS 2020,* (pp. 267–287). Springer.

Liu, C. W., Huang, P., & Lucas, H. C. (2018). IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. In Y. J. Kim, R. Agarawal & J. K. Lee (Eds.), *ICIS 2017: Transforming Society with Digital Innovation,* (pp. 1–18). Seul, South Korea: Association for Information Systems.

Marcikić, A., & Radovanov, B. (2011). A Decision Model for Outsourcing Business Activities. *International Symposium Engineering Management and Competitiveness*, 69–74.

MarketsAndMarkets. (2020). *Managed Security Services Market by Type (Managed IAM, Antivirus/Antimalware, SIEM, and UTM), Deployment Mode, Organization Size, Vertical (BFSI, Government, Retail, Healthcare, Telecom, Utilities, and Manufacturing), and Region - Global Forecast to 2025.* Retrieved from: https://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html

Moisiadis, F. (1999). Case Study on the Use of Scaling Methods for Prioritising Requirements. *INCOSE International Symposium*, *9*(1), 1451–1457.

Pakpahan, J., Eryadi, R. A., Budiman, A., Sunandar, N., Syahid, L. M., & Shihab, M. R. (2021). Critical Success Factors of IT Outsourcing in Indonesian Public Sectors: A Case Study at Employment Social Security Agency. *ICOIACT 2021 - 4th International Conference on Information and Communications Technology: The Role of AI in Health and Social Revolution in Turbulence Era*, (pp. 47–52). Online: IEEE.

Ponemon Institute. (2019). *The Cost of Third-Party Cybersecurity Risk Management.* Retrieved from: https://www.cybergrx.com/resources/research-and-insights/ebooks-and-reports/the-cost-of-third-party-cybersecurity-risk-management

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A european perspective. In P. Mori, S. Furnell & O. Camp (Eds.). *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy,* (pp. 426–431). Madeira, Portugal: Springer.

Popp, N., Jensen, J. A., McEvoy, C. D., & Weiner, J. F. (2020). An examination of the effects of outsourcing ticket sales force management. *International Journal of Sports Marketing and Sponsorship*, *21*(2), 205–223.

Prakash, S., Soni, G., Mittal, S., & Singh Rathore, A. P. (2014). Information Risks Modeling in e-business Supply Chain using AHP. *In Recent Advances in Engineering and Computational Sciences (RAECS),* (pp. 1-5). Chandigarh, India: IEEE.

Rajaeian, M. M., Cater-Steel, A., & Lane, M. (2015). IT outsourcing decision factors in research and practice: A case study. In F. Burstein, H. Scheepers & G. Deegan (Eds.). *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*, (pp. 1–12). Adelaide, Australia: University of South Australia.

Ren, Z. J., & Zhou, Y. P. (2008). Call center outsourcing: Coordinating staffing level and service quality. *Management Science*, *54*(2), 369–383. https://doi.org/10.1287/mnsc.1070.0820

Russo, R. D. F. S. M., & Camanho, R. (2015). Criteria in AHP: A systematic review of literature. *Information Technology and Quantitative Management*, *55*, 1123–1132. https://doi.org/10.1016/j.procs.2015.07.081

Saaty, T. L. (1980). *The Analytic Hierarchy Process*. McGraw Hill.

Saaty, T. L. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, *48*(1), 9–26. https://doi.org/10.1016/0377-2217(90)90057-I

Saaty, T. L., & Tran, L. T. (2007). On the invalidity of fuzzifying numerical judgments in the Analytic Hierarchy Process. *Mathematical and Computer Modelling*, *46*(7–8), 962–975. https://doi.org/10.1016/j.mcm.2007.03.022

Shahrasbi, A., Shamizanjani, M., Alavidoost, M. H., & Akhgar, B. (2017). An aggregated fuzzy model for the selection of a managed security service provider. *International Journal of Information Technology and Decision Making*, *16*(3), 625–684. https://doi.org/10.1142/

S0219622017500158

Sung, W., & Kang, S. Y. (2017). An empirical study on the effect of information security activities: Focusing on technology, institution, and awareness. In C. C. Hinnant & O. Adegboyega (Eds.). *ACM International Conference Proceeding Series*, (pp. 84–93). New York, New York: Association for Computing Machinery.

Wang, G., Qin, L., Li, G., & Chen, L. (2009). Landfill site selection using spatial information technologies and AHP: A case study in Beijing, China. *Journal of Environmental Management*, *90*(8), 2414–2421. https://doi.org/10.1016/j.jenvman.2008.12.008

Wang, J. J., Lin, Z. K., & Zhang, G. Q. (2008). A decision model for IS outsourcing based on AHP and ELECTREIII. In *2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008*, (pp. 1–4). Dalian, China: IEEE.

Wu, Y., Duan, J., Dai, T., & Cheng, D. (2020). Managing security outsourcing in the presence of strategic hackers. *Decision Analysis*, *17*(3), 235–259. https://doi.org/10.1287/deca.2019.0406

Wu, Y., Fung, R. Y. K., Feng, G., & Wang, N. (2017). Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Computers and Industrial Engineering*, *110, 1-12*. https://doi.org/10.1016/j.cie.2017.05.018

Zammani, M., Razali, R., & Singh, D. (2019). Factors contributing to the success of information security management implementation. *International Journal of Advanced Computer Science and Applications*, *10*(11), 384–391. https://doi.org/10.14569/IJACSA.2019.0101153

Zúñiga, A. R. R., & Jaatun, M. G. (2016). Passing the buck: Outsourcing incident response management. In *Proceedings of 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015*, (pp. 503–508). Vancouver, Canada: IEEE.

Luka Jelovčan is a project manager at SGB d.o.o., Ljubljana, Slovenia. His primary research interests are in human factors in cybersecurity, corporate risk management, and enterprise information systems management. ORCID: 0000-0003-0131-9876

Anže Mihelič is a Ph.D. candidate at the Faculty of Law and Faculty of Computer and Information science, both at the University of Ljubljana. He is employed at the University of Maribor, Faculty of Criminal Justice and Security. His primary research interests are human aspects of information- and cyber-security, privacy law, adoption of new technologies, and secure software development methodologies. ORCID: 0000-0002-5925-4262

Kaja Prislan holds a Ph.D. in security studies. She is an assistant professor at the University of Maribor, Faculty of Criminal Justice and Security. Her research interests include information security management, behavioral information security, and security in (smart) communities. ORCID: 0000-0002-8474-7122