mathematics

MDPI

Article

A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment

Davor Maček *, Ivan Magdalenić and Nina Begičević Ređep *

Faculty of Organization and Informatics Varaždin, University of Zagreb, Pavlinska 2, 42000 Varaždin, Croatia; ivan.magdalenic@foi.unizg.hr

* Correspondence: davor.macek@foi.unizg.hr (D.M.); nina.begicevic@foi.unizg.hr (N.B.R.)

Abstract: One of the important objectives and concerns today is to find efficient means to manage the information security risks to which organizations are exposed. Due to a lack of necessary data and time and resource constraints, very often it is impossible to gather and process all of the required information about an IT system in order to properly assess it within an acceptable timeframe. That puts the organization into a state of increased security risk. One of the means to solve such complex problems is the use of multicriteria decision-making methods that have a strong mathematical foundation. This paper presents a hybrid multicriteria model for the evaluation of critical IT systems where the elements for risk analysis and assessment are used as evaluation criteria. The iterative steps of the design science research (DSR) methodology for development of a new multicriteria model for the objectives of evaluation, ranking, and selection of critical information systems are delineated. The main advantage of the new model is its use of generic criteria for risk assessment instead of redefining inherent criteria and calculating related weights for each individual IT system. That is why more efficient evaluation, ranking, and decision-making between several possible IT solutions can be expected. The proposed model was validated in a case study of online banking transaction systems and could be used as a generic model for the evaluation of critical IT systems.

Keywords: information security; risk assessment; multicriteria decision-making; hybrid model; criteria dependence; critical IT systems

Citation: Maček, D.; Magdalenić, I.; Begičević Ređep, N. A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment. *Mathematics* **2021**, *9*, 1045. https://doi.org/10.3390/math9091045

Academic Editor: Antonio Francisco Roldán López de Hierro

Received: 13 April 2021
Accepted: 29 April 2021
Published: 6 May 2021

1. Introduction

The main goals of information security and all business decision-makers are to defend their organizations and the capability to protect associated IT assets, as well as ensure the confidentiality, integrity, and availability (C-I-A) of information and the information systems that retrieve, process, store, and distribute that information [1]. Thus, security risks are also inevitably involved. According to the authors of [2], risk management is recognized as a key component of managing IT security risks. Security risks can have different dimensions and effects with the possibility of occurring at different levels, and also require their own specific preventative countermeasures to be implemented at any possible level [3]. Information security risks are an omnipresent phenomenon today, because there is no organization that is not faced with certain security threats (e.g., malware, phishing, spoofing, eavesdropping, denial of service, etc.) and consequently also related risks to their IT systems (e.g., IT operational, legal, regulatory, financial, or reputation risk). There are many external factors such as emerging cyber-attacks on organizations, especially financial institutions and their clients [4–6], where extremely dangerous WannaCry and Petya attacks must be highlighted [7,8]. There has been an uptrend in the number of security threats and cyber-attacks on financial institutions; according to the Verizone Report [9], around 86% of successful cyber-attacks are financially motivated. Furthermore, according to the IMF [10], the risk of cyber-attacks is now perceived as the most important risk in the financial sector.

Additionally, the number of ICT security threats and related cyber attacks has significantly increased during the COVID-19 pandemic [11,12].

The management and evaluation of IT security risks is a highly critical process and actually comprises a set of related activities to control and manage risks to the information system. The major objective of this process is to reduce risks to an acceptable level [13,14] depending on the level of risk appetite that the management of the organization is ready to accept [15]. One of the means to adequately manage risks in financial institutions is to assess and select an appropriate IT solution in order to meet primarily business, but also a number of regulatory, compliance and security requirements. However, making a decision about the security posture and choosing the appropriate IT solution in the organization is often a complex, time-consuming, and costly process. Due to the growing trend of increasing security threats and discovery of new vulnerabilities, and frequently the lack of time and resources in organizations to efficiently respond to information systems risks, addressing the most critical security risks and assessing critical IT systems becomes an essential problem. This research deals with the problem of multicriteria decision-making in conditions of uncertainty, i.e., the risk of information security in the domain of critical IT systems in a financial institution within the context of assessing and selecting an appropriate IT solution.

Certain shortcomings have been identified in the existing methods of addressing information security risks and consequently the evaluation of IT solutions, and therefore there is a need for a more efficient way to evaluate critical IT systems. In this paper, we propose a mathematical model for the evaluation of critical IT systems using multicriteria decision-making with elements for risk analysis and assessment, which should make such evauations more efficient (in terms of costs and time). The greatest emphasis in the new multicriteria model is on the use of generic risk criteria as evaluation elements instead of recurrent identification of inherent (i.e., common, typical) criteria and demanding calculation of related weights for every particular IT system. Thus, more effective and efficient evaluations of the security posture and consequently, informed decision-making regarding the selection of adequate IT systems, can be expected. Additionally, the great contribution of the hybrid model is that interdependencies and influences between the elements for information security risk assessment are taken into account because such complex and variable connections are usually neglected in many other models, especially when solely the AHP method is used. This paper provides a unique mathematical multicriteria model that should be suitable for the selection of appropriate IT hardware, software solutions, cryptographic algorithms or protocols, etc.

The rest of this paper is organized as follows. Section 2, presents the research questions and meaningful related works along with a systematic literature review. In Section 3, the research problem is observed in more detail. In Section 4, the research goals, hypotheses, related metrics, and research methodology are presented. A hybrid mathematical multicriteria model is presented in Section 5, while validation of the model (case study) is covered in Section 6. Section 7 comprises discussions of the model and potential future research. Finally, Section 8, presents certain conclusions.

2. Related Works

Thes incentive for this research arose from work and research experiences where the author identified an issue in the absence of an effective (in terms of costs and time) model or method for the evaluation of critical IT systems in a financial institution in order to better address security risks, and also be able to make an appropriate decision on the security posture for a particular IT system, as well as to finally assist in selection of an appropriate critical IT solution. The introduction to a new mathematical model and planned research was already presented in a previous paper [16]. In this research phase, the following research questions (RQ) were defined:

(1) RQ1: How to enable more efficient decision-making on the security posture and selection of an adequate critical information system for a financial institution?

(2) RQ2: Which elements for security risk analysis and assessment are appropriate and relevant to the development of a hybrid multicriteria model for the evaluation and selection of critical IT systems in order to more efficiently make informed decisions about the observed critical IT system in a financial institution?
(3) RQ3: For which critical IT systems is the designed mathematical multicriteria model applicable and valid?

In order to assure relevant answers to these research questions, it was necessary to review the literature and analyze existing methods and models within the areas of multicriteria decision-making and risk assessment that were used for the assessment of information systems. Any review of the literature must be conducted entirely and impartially in order to gain confident scientific value. The literature review from index citation databases was conducted by enforcing guidelines for systematic literature review (SLR) in software engineering [17]. SLR presents a formalized and repeatable process for the documentation of substantial knowledge in a specific research field, in this case the application of multicriteria decision-making (MCDM) methods in the area of information security risk.

The SLR research [18] with very rigorous criteria defined finally discovered 65 relevant papers where various MCDM methods and techniques were used for the purpose of information security risk analysis, assessment, and management. The literature review indicated that in many analyzed studies, a certain level of quantification was demanded for the evaluation and ranking of IT security risks, risk factors, or software solutions. So, the use of a quantitative MCDM method was required. The SLR survey demonstrated that the international standard ISO/IEC 27005 was dominantly analyzed and served as a landmark and cornerstone for the purposes of information security risk analysis, assessment, treatment, and overall management [19,20]. According to [21], ISO/IEC 27005 is the most complete ISRA method. Other widely accepted ISRA (Information Security Risk Assessment) methods and standards [22] are NIST SP 800-30, ISO/IEC 31010:2009, CRAMM, CORAS, and OCTAVE. The same survey also revealed the frequency of use of MCDM methods and techniques in theISRA domain, where the most utilized MCDM method for the purposes of IT security risk analysis and assessment was the Analytic Hierarchy Process (AHP) [23]. This could be attributable to the relative ease of use of the AHP method itself and its strong popularity among many researchers. Other frequently used MCDM methods in the ISRA domain are the ANP (Analytic Network Process), DEMATEL, and TOPSIS. The DEMATEL [24] was used to calculate the influence weights, while the ANP [25,26] was used to calculate interdependencies of the evaluation elements [27–29]. The SLR discovered that ISRA elements or C-I-A attributes were used and integrated within some MCDM methods in a small number of studies [28,30–35].

Besides the conducted SLR, there were some newer, valuable papers that also explored the development of certain hybrid models and methods, e.g., a model for complex benchmarking of MCDA methods [36], the consensus-based group decision-making (GDM) approach using the AHP model in an incomplete environment exploiting fuzzy information [37], and an ITARA-TOPSIS model as an assessment tool for system risk identification where the determination of risk factors is based on the failure mode and effect analysis (FMEA) theory [38].

The conclusion was that the very narrow field of risk assessment methods for the specific purpose of assessment of critical IT solutions with the use of MCDM with strong mathematical foundations had not yet been investigated thoroughly enough in scientific studies. This actually highlights certain shortcomings in the research field, as there has been no contribution to the development of any model that could serve for solving the observed complex decision-making problem. However, these findings were also a notable roadmap and have had a strong impact on further research aimed at extending the core ISRA attributes, defining their influences and interdependencies, and then integrating those attributes within an appropriate MCDM method for the purpose of evaluating critical IT systems in a more efficient and accurate manner. With the completion of SLR research, a

need for a new model was identified for the specific purpose of more efficient evaluations of critical IT systems by using multicriteria decision-making with the integration of attributes for risk analysis and assessment. Such a new model should be a significant contribution to the field of information security, specifically the risk management domain, and should facilitate making informed decisions on the security posture of critical IT systems.

3. Problem Observation

For any decision-making problem, it is also necessary to choose the appropriate MCDM method that will be used to calculate the criteria weights. The most important characteristics that a given MCDM method must support when calculating the weights of ISRA evaluation criteria, and that the new hybrid model must also take into account, are two dimensions for each observed ISRA criterion: the importance or comparisons of the criteria themselves with regard to the decision goal, and the mutual influences and dependencies (i.e., feedback) between the defined criteria [39]. The AHP certainly takes into account the importance of the criteria in relation to the decision goal, and the ANP takes into account the influences (dependencies) between the criteria themselves. The conducted SLR [18] showed a certain level of use of the ANP despite the complexity of its application, and often in combination with the DEMATEL [40–42]. Further, it showed how a goal cluster can be introduced in the ANP [28,43]. However, a detailed mathematical analysis of the ANP [44] showed that comparisons of the criteria with respect to the goal have no effect on the final weights of the evaluation criteria, and thus very complex and time-consuming calculations become completely unnecessary. In addition, in the ANP, the criteria and alternatives are interdependent, which is to be avoided and also represents a certain limitation for the development of a new model for the evaluation of critical IT systems. Due to the above, it is clear that the most commonly used MCDM methods, such as AHP, ANP, TOPSIS, or VIKOR (discovered during the SLR), are not quite suitable for solving the observed complex research problem. Therefore, the proposal was to use SNAP (social network analytic process) as the MCDM method that best corresponds to the required characteristics.

The SNAP [42,44] is a completely new method for multicriteria decision-making developed for the needs of analysis and solving complex decision-making problems based on the ANP method and measures of centrality taken from the method for social network analysis (SNA). In the work [44], it was mathematically proved that the SNAP method has none of the limitations that the AHP (no dependence between the criteria) or the ANP (neglected importance of criteria with respect to goal, interdependence of criteria and alternatives, as well as high user complexity due to excessive number of comparisons in pairs) methods have. Moreover, it was shown that the SNAP method was significantly easier to use compared to the ANP. Various SNAP versions are available, but for the purposes of this research, the SNAP11 method with PageRank centrality to calculate generic ISRA criteria weights was used. PageRank is an algorithm used by Google Web Search to rank web pages based on search results. PageRank is a way of measuring the importance of a website. The PageRank algorithm for calculating PageRank centrality is based on the assumption that the relevant website is the one to which a large number of other websites refer to, taking into account the relevance, importance, or popularity of a particular page [45,46].

In his work [47], B. Roy points out that the choice of MCDM method is an extremely important element in solving decision-making problems, and in order to obtain an appropriate solution to a defined problem, the decision maker must also select and apply the appropriate method. According to [48,49], the decision makers are often unable to justify their choice of method used to solve certain decision situations, so the choice of MCDM method is mostly arbitrary and motivated by the decision maker's knowledge of the chosen method or availability of software support for the method itself. Similar problems exist with the selection of MCDM software, where decision makers most often choose decision support software that they are familiar with [50]. So, there are situations where a particular

MCDM method is not selected to solve a specific problem, but the decision problem is actually adapted to the selected MCDM method and associated software. The problem of selecting the appropriate MCDM method for a particular decision-making situation is evident from the fact that different methods can give different results for the same observed situation. So, the choice of MCDM method depends on the characteristics of the decision problem itself.

Thus, it was necessary to conduct additional research to see if there was a defined methodology, framework, or specific set of instructions for selecting an adequate MCDM method, and also given the fact that there are already calculated weights of generic risk criteria obtained by the SNAP11 method. Certain significant studies were found to deal with the problem of selection and systematization of MCDM methods for specific decision-making problems [48,51]. However, we found no other relevant research regarding the selection of an adequate MCDM method in the context of assessing the security state of an information system and/or information security risks. So, as the starting point for the selection of a relevant MCDM method in which the weights of the generic risk criteria obtained by the SNAP11 method would be integrated, a general framework for the selection of the MCDM method that is independent of the problem domain was used [52]. The proposed framework is based on determining a set of characteristics of available MCDM methods and the characteristics of a particular decision problem, and is an attempt to resolve uncertainties in the process of selecting an appropriate MCDM method. The framework initially requires that the decision maker (DM) define only the so-called general descriptors (c) of a particular decision problem. Given the characteristics of decision-making problems related to the evaluation, ranking, and selection of critical IT solutions using multicriteria decision-making with elements for risk analysis and assessment, which is the subject of this paper and research, the input parameters (i.e., descriptors) were as follows:

(1) c1: Criteria weights: Yes—obtained by SNAP11 method
(2) c1.1: Type of criteria weight: Relative
(3) c2: Type of scale for evaluating alternatives: Relative
(4) c3: Uncertainty in the decision-making problem: No
(5) c4: Type of decision-making problem: Ranking and choice
(6) c4.1: Ranking type: Complete.

By integrating the characteristics of these descriptors into the software support [53] developed specifically for the proposed general framework, we obtained the following possibilities for the selection of an adequate MCDM method: AHP, ANP, DEMATEL, MACBETH, and REMBRANDT. The rationales regarding the choice of appropriate MCDM method for the evaluation of critical IT systems will follow in the chapter related to the presentation of the new multicriteria model.

4. Research Goals, Hypotheses, and Methodology

4.1. Research Goals and Hypotheses

The scientific research presented in this paper has several goals that can be separated into one main (general) goal and three specific goals. The general goal is the following:

To develop a mathematical model for making an informed decision on the security posture of critical information systems in a financial institution and increasing the efficiency and quality of the assessment and selection process of such critical systems.

The defined specific goals (SG) are the following:

(1) SG1: To conduct a detailed and systematic review of the research area in order to determine which methods and techniques for risk assessment and multicriteria decision-making are currently used for the evaluation, ranking, and selection of information systems.
(2) SG2: To develop a multicriteria hybrid model with relevant elements for risk assessment as generic criteria for the purpose of evaluation, ranking, and selection of critical information systems using multicriteria decision-making methods.

(3) SG3: To validate a new multicriteria hybrid mathematical model.

The following two scientific hypotheses were set:

Hypothesis 1 (H1). *A mathematical multicriteria model for the assessment, ranking, and selection of critical information systems with generic criteria for risk analysis and assessment is valid.*

This hypothesis is related to the fulfilment of specific goal SG2 and provides an answer to the research question RQ1, where the solution of the observed problem proposes the development of a multicriteria model for evaluation, ranking, and selection of critical IT systems with generic risk criteria. The validity of the model will be determined by the validation process in the case study by applying the defined metric M1, which achieves specific goal SG3 and provides an answer to research question RQ3. Additionally, the development of a multicriteria model with appropriate elements for risk analysis and assessment provides an answer to research question RQ2.

Hypothesis 2 (H2). *A mathematical multicriteria model with generic risk criteria in the decision-making process is more efficient than a model with inherent (common) attributes.*

This hypothesis is directly related to the fulfilment of specific goal SG3 (validation of the new model) and provides an answer to the research question Q3 about the applicability and validity of the model itself. The effectiveness of the model will be determined by a validation process in a case study using a defined M2 metric.

The metrics applied in the research during the validation process in order to achieve the main goal, which is to more efficiently make an informed decision about the security posture and selection of a critical information system in a financial institution, are as follows:

(1) M1: The deviation in the ranking of critical IT solutions for the results obtained by the new hybrid model with generic risk criteria in comparison to the ranking results using the inherent attributes of the observed information systems from the case study during the validation process.
(2) M2: The difference in the number of full-time equivalents (FTEs) required for the evaluation of critical information systems according to the new proposed hybrid multicriteria model with generic risk criteria in comparison to the evaluation of such IT systems with inherent criteria.

If the new multicriteria model with generic risk criteria points to the same ranking of information systems as in the case when inherent (common) attributes are used for the observed IT system using one of the chosen methods for multicriteria decision-making, while also spending less time and resources, then the defined main (general) goal is achieved.

4.2. Research Methodology

The research paradigm followed in this research was the design science research methodology (DSRM), which is used for scientific research purposes primarily in engineering and information systems. Research using this paradigm involves creating new knowledge by designing new or innovative artifacts (things or processes) and analyzing the use and/or performance of such artifacts—to improve and understand the behavior of certain aspects of the information system. The artifacts created in the design science research process include, but are not limited to, algorithms, human/computer interfaces, and system design methodologies or languages [54,55].

Figure 1 shows all the research phases as well as the scientific methods used for research purposes. By finishing the systematic literature review, specific goal SG1 is achieved, thus enabling one to move forward with the research and use the Delphi technique and statistical methods in order to obtain the exact ISRA elements that will be used as generic evaluation criteria within the new multicriteria model. According to the guidelines for the implementation of design science research [56], an additional activity is carried out in the research methodology, namely the creation of a knowledge base [57], where the goal is to

collect all the possible knowledge in the research domains. Collected knowledge serves as an indispensable input for development of a new mathematical multicriteria model and also provides an answer to the research question RQ2 about ISRA evaluation criteria. When the new multicriteria model with all the relevant generic ISRA criteria is developed and demonstrated, then specific goal SG2 is achieved, thus allowing the move to the next crucial research phase of model evaluation in order to achieve specific goal SG3 and prove the defined hypotheses.

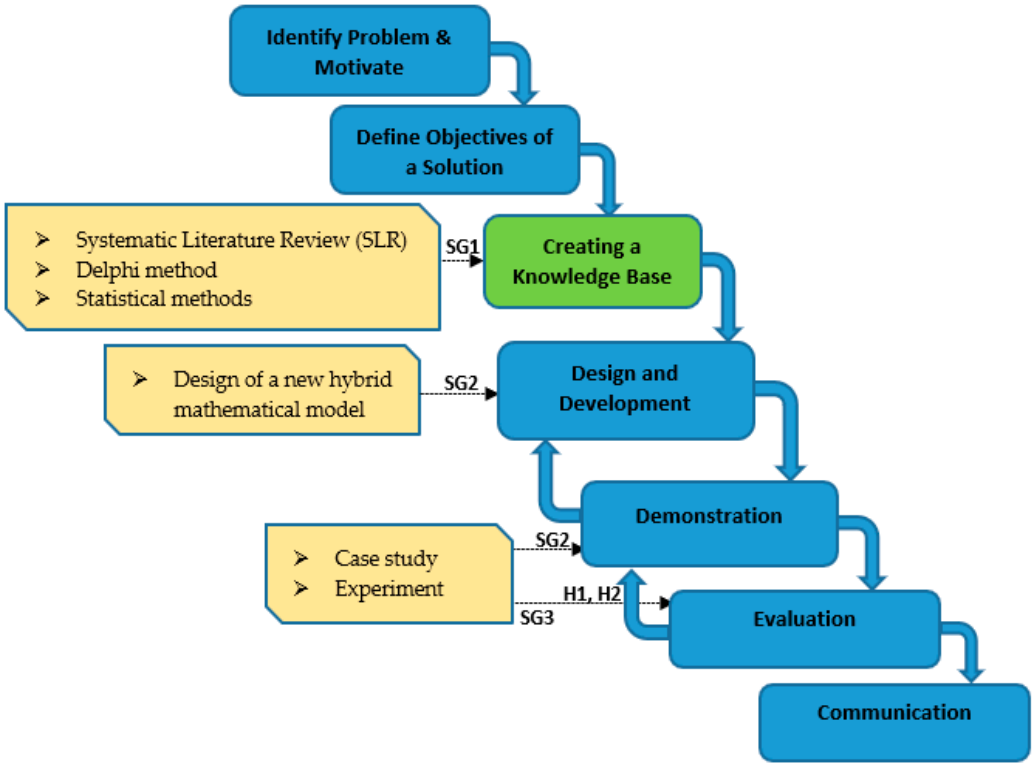

Figure 1. Research process and scientific methods.

5. A Hybrid Mathematical Multicriteria Model

In this section, the entire research process and a new hybrid multicriteria model with strong mathematical foundation for the evaluation of critical IT systems are presented.

5.1. Identification of Risk Assessment Elements

After finishing with SLR and discovering which MCDM methods should be considered as relevant for the new multicriteria model, this research phase identifies all the necessary information security risk assessment elements that are used as the evaluation criteria for critical IT systems.

This research was performed with the Delphi technique, where IT security professionals were asked to provide their opinions on the risk assessment elements that will be used for the evaluation of critical IT systems. IT security experts with more than 15 years of average experience in the field of IT and IT security from various countries and different European financial institutions holding relevant industry certifications (e.g., CISSP, CISM, CRISC, CEH, etc.) were queried. Each IT security expert held at least a bachelor's or master's degree, while 5 respondents also had PhDs. The questionnaire (shown in Figure A1) was initially sent via e-mail to 78 IT security experts and managers; properly completed forms were returned by 38 respondents from 12 European countries. Experts were asked to express their own views on the ISRA criteria (proposed on the basis of the ISO/IEC 27005 standard), and also to possibly propose and explain the need for additional risk

assessment elements that could become an integral part of the new multicriteria model for the evaluation of critical IT systems.

In the second round of the Delphi research, 33 valid responses were received from 38 respondents. The answers were related to the measurement of attitudes for critical elements for the analysis and assessment of information security risks and were designed as semantic ordinal scale of the Likert type, where good practices [58] were also used in compiling the questionnaire. The questionnaire and the results obtained by Delphi technique are presented in Appendix A.

For computations and interpretations of results, central tendency measures (arithmetic mean and mode) and variance level measures (standard deviation and coefficient of variation) were used as supporting statistical methods. According to [59], consensus in the Delphi technique is reached if the following conditions are met: the standard deviation value is less than 1.5 and more than 51% respondents affirmatively (or negatively) expressed their views regarding certain elements, objects, or phenomena. In this research, the standard deviation value was less than 0.95 for each observed element and the incidence of positive agreement attitude (4 agreed and 5 strongly agreed) was much higher than the required 51% of respondents for the 5 proposed ISRA elements.

In the second round of the Delphi research, exploitability (E) was added as an additional element for evaluation purposes because it was proposed in the first Delphi round by several IT security experts. However, a majority of other IT security professionals expressed the view that the exploitability element was conceptually part of the probability with less of importance and thus would add redundancy and increase the complexity of the new model, which is certainly to be avoided given the defined H2 hypothesis about greater efficiency of the new multicriteria model. Therefore, the exploitability element was not part of the model as an evaluation criterion, but rather as a meaningful impact factor that should be considered for probability and vulnerability ISRA criteria.

Figure 2 presents the proportions of IT security expert attitudes regarding the ISRA elements as evaluation criteria of IT systems. Finally, after two rounds of the Delphi research, the following risk assessment elements were identified as sufficient and also comprehensive enough to be used as evaluation criteria for the purpose of evaluating critical IT systems: threat (T), vulnerability (V), probability (P), consequence (C), and resiliency (R).

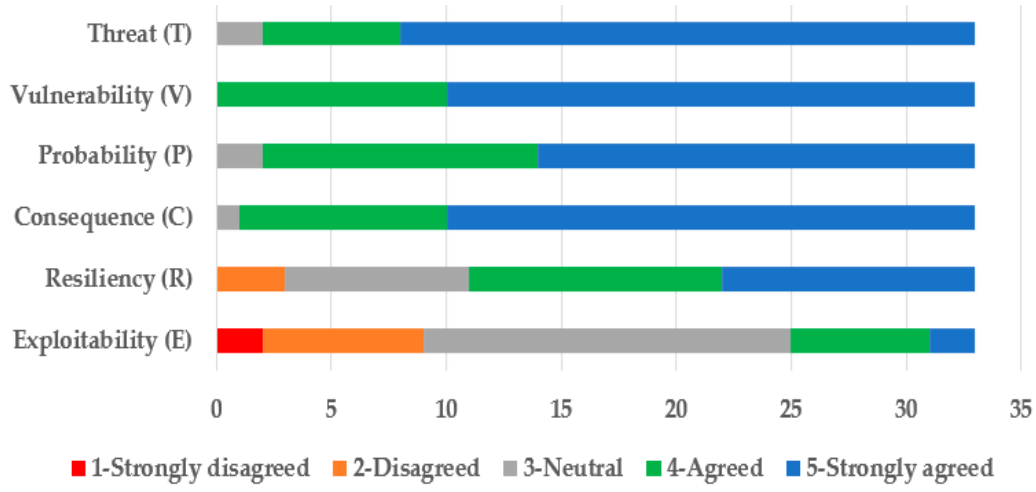

Figure 2. Experts' attitudes on the ISRA criteria.

5.2. Determining the Weights of Generic Risk Assessment Criteria

The next qualitative DSRM research step was to calculate the weights of identified criteria for risk assessment.

Because the SNAP11 method [44] was chosen as the appropriate MCDM method for calculating ISRA criteria weights, two important input components for implementation were needed: influences (dependencies) between the elements and the weights of the criteria in relation to the decision goal. Data collection was once again performed by querying IT security experts, and 23 respondents from various European financial institutions provided their valuable judgments in two phases.

The steps of the SNAP11 method are as follows:

1. The first input element is a matrix Z of weight relations of influence (aggregation of collected opinions of IT security experts and calculation of the average matrix Z—the first step in the DEMATEL method;
2. Calculation of the average sums of each column and identifying the column with the largest average sum;
3. Calculation of the normalized matrix S of the weight relations of the influence in such a way that each element from the matrix Z is divided by the value of the identified maximum sum of the column increased by 1;
4. Defining a matrix E—a matrix of size n that has all values equal and is $\frac{1}{n}$;
5. Calculation of the matrix G according to the formula G = (0.85·S) + (0.15·E). Various studies have tested different damping factors, but in general, according to the authors of the Google PageRank algorithm [60], this factor is around 0.85;
6. Calculation of the matrix I − G (I represents the identity/unit matrix);
7. Inverse matrix calculation $(I - G)^{-1}$;
8. Multiplication of the matrix G by the inverse matrix $(I - G)^{-1}$;
9. Calculating the values of P_DO, P_DI and their difference r (i.e., $P_DO - P_DI$) for the matrix from the previous step, where P_DO—outgoing centrality, i.e., the sum of the rows in the final matrix P_DI—incoming centrality, i.e., the sum of the columns in the final matrix;
10. Adding the constant c to the difference r, where

$$c = \max_{i=1}^{n}\{P_DO(i) - P_DI(i)\} - \min_{i=1}^{n}\{P_DO(i) - P_DI(i)\} \quad (1)$$

11. Calculating the average of the weights obtained from the previous step with the weights of the criteria in relation to the decision goal.

Phase 1: Security experts provided their ratings on the DEMATEL scale (0–4) for the influences (dependencies) between previously identified elements for risk analysis and assessment.

Figure 3 shows the matrix that was sent to IT security professionals for completion. After collecting the answers, aggregation of received values was performed and all the other necessary computations were conducted according to the steps of the SNAP method [44]. The result of this step were the weights of the ISRA criteria corresponding to the SNAPv12 method, which is shown in Table 1.

Risk criteria influences and dependencies	Threat (T)	Vulnerability (V)	Probability (P)	Consequence (C)	Resiliency (R)
Threat (T)	0				
Vulnerability (V)		0			
Probability (P)			0		
Consequence (C)				0	
Resiliency (R)					0

0 (no influence)
1 (low influence)
2 (medium influence)
3 (high influence)
4 (very high influence)

Figure 3. Matrix for estimating influences and dependencies between ISRA criteria.

Table 1. Weights of generic ISRA elements obtained by SNAP12 method.

ISRA Criteria	Weight (SNAP12)
Threat (T)	0.198096379
Vulnerability (V)	0.318888835
Probability (P)	0.143692265
Consequence (C)	0.118888835
Resiliency (R)	0.220433685

However, this SNAPv12 method does not take into account comparisons of criteria in relation to the decision goal, which is important in this case due to the definition of the research problem. So, phase 2 is needed to calculate the final weights of generic ISRA criteria using the targeted SNAPv11 method.

Phase 2: Security experts provided their ratios on the importance of risk criteria in relation to the goal of decision-making using the AHP, because the AHP is an integral part of the SNAP11 steps. The identified ISRA criteria are divided into 2 clusters: the Risk cluster which contains 4 standard criteria for risk analysis and assessment (probability, threat, vulnerability and consequence, all according to the international standard ISO/IEC 27005) and the Resiliency cluster containing only the Resiliency element itself. The comparisons were done between the elements inside the Risk cluster and between the defined two clusters. The standard Saaty scale [23] was used for pairwise comparisons, i.e., defining the importance between ISRA criteria. The results obtained within this subphase were as follows.

Table 2 shows the ISRA criteria weights obtained by input judgments of IT experts and necessary calculations with the AHP method. It iss actually an intermediate step in order to calculate the final ISRA criteria weights. And to do so, it was necessary to calculate the arithmetic mean (Table 3) of the values obtained by the SNAPv12 method and the AHP intermediate step, as presented in previous tables.

Table 2. Weights of generic ISRA criteria obtained by the AHP.

ISRA Criteria	Weight (AHP)
Threat (T)	0.105824012
Vulnerability (V)	0.186796789
Probability (P)	0.057177557
Consequence (C)	0.196417034
Resiliency (R)	0.453784608

Table 3. Weights of generic ISRA criteria obtained by SNAP11 method.

ISRA Criteria	Weight (SNAP11)
Threat (T)	0.151960196
Vulnerability (V)	0.252842812
Probability (P)	0.100434911
Consequence (C)	0.157652935
Resiliency (R)	0.337109146

The final weights of the generic criteria for information security risk analysis and assessment obtained by the SNAP11 method were as follows.

These weights of the generic risk criteria from Table 3 are used as a multiplication vector together with the eigenvector values obtained during the evaluation of critical information systems (case study) according to defined ISRA criteria in the research phase validation of the model. These generic ISRA criteria weights are calculated just once, whereas for the model with inherent criteria, it is necessary to identify and calculate such criteria every time for specific IT systems that are to be evaluated, which is a quite intensive process in terms of time and resources.

Detailed procedures for calculating the weights of generic ISRA criteria using the SNAP11 method can be found in Appendix B.

Additionally, calculations of reference rankings for generic ISRA criteria were performed by using r_w and *WS* coefficients. WS is a new coefficient of rankings similarity that can be used in decision-making problems [61]. In order to perform the calculations, rankings of SNAP12 ISRA criteria weights were used as reference rankings (R_x), where the vulnerability (V) criterion has the largest weight and is thus ranked first (1), then the resiliency (R) criterion comes with its second ponder and is thus ranked second, etc. The reason to use ISRA criteria weights obtained with the SNAP12 method comes from the logic because SNAP12 weights are the first ones calculated and serve as a precondition in order to obtain the required SNAP11 weights for generic ISRA criteria.

From Table 4 it can be seen that there is a relatively low correlation between criteria rankings when different MCDM methods are used to obtain the weights of generic ISRA criteria; this is actually expected. Furthermore, the ***WS*** coefficient seems to be much more consistent and precise for measurements of the similarity of rankings for generic ISRA criteria.

Table 4. Summary of reference rankings ($\boldsymbol{R_x}$) for ISRA criteria.

ISRA Criteria	SNAP12 Rank (R_x)	AHP Rank ($R_y^{(1)}$)	SNAP11 Rank ($R_y^{(2)}$)
Threat (T)	3	4	4
Vulnerability (V)	1	3	2
Probability (P)	4	5	5
Consequence (C)	5	2	3
Resiliency (R)	2	1	1
Coefficients	r_w	0.216667	0.650000
	WS	0.559896	0.692708

5.3. Selection of MCDM Method for Evaluation of Alternatives

After obtaining the weights of the generic ISRA criteria by the SNAP11 method, it is now necessary to include those criteria weights in the appropriate MCDM method in order to finally use the defined generic ISRA criteria and associated weights to evaluate alternatives (i.e., critical IT systems) in the case study.

Given the specific problem and requirements of this research, where dependencies between the evaluation criteria and also the importance of the criteria in relation to the decision goal must be taken into account, and the fact that during the process of calculating the weights of generic risk criteria the AHP has already been used in one phase (as an integral part of the SNAP11 calculations), the selection of the AHP method seems quite reasonable for the purpose of evaluating critical IT systems among other available MCDM methods already obtained with a general framework for selection of the MCDM method [53] according to the defined parameters. The rationales for using the AHP as a method for the purposes of evaluating critical IT systems are as follows: It allows the structuring of decision-making problems, support for qualitative and quantitative scales of criteria, group decision-making, sensitivity analysis, consistency checks in decision-maker assessments, ranking of alternatives, and broader software support [23,62,63].

5.4. Demonstration of the New Hybrid Multicriteria Model

Based on the results of the conducted research on the most important elements for risk assessment arising from the Delphi research technique, then the analysis of MCDM methods, identification of links between ISRA elements and defining their weights, this section presents the final model for evaluation of critical IT solutions.

First, the high-level components will be presented to summarize the research process that led to the new hybrid multicriteria model.

Figure 4 shows the main high-level components used to build the new multicriteria model. These components actually correspond to research phases, where the Delphi

technique was used for identification of core ISRA elements, and the DEMATEL method was used to obtain influences and dependencies between ISRA elements that served later on as an initial input into the SNAP method by which ISRA criteria weights were calculated. Finally, the AHP was used for the assessment of critical IT systems with generic ISRA attributes as evaluation criteria.

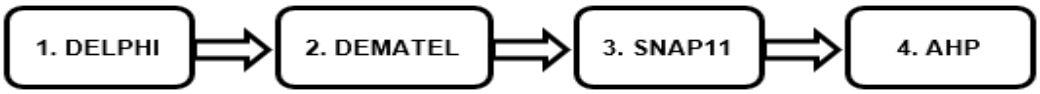

Figure 4. High-level components used in development of a new multicriteria model.

Finally, in Figure 5, a new multicriteria model is presented.

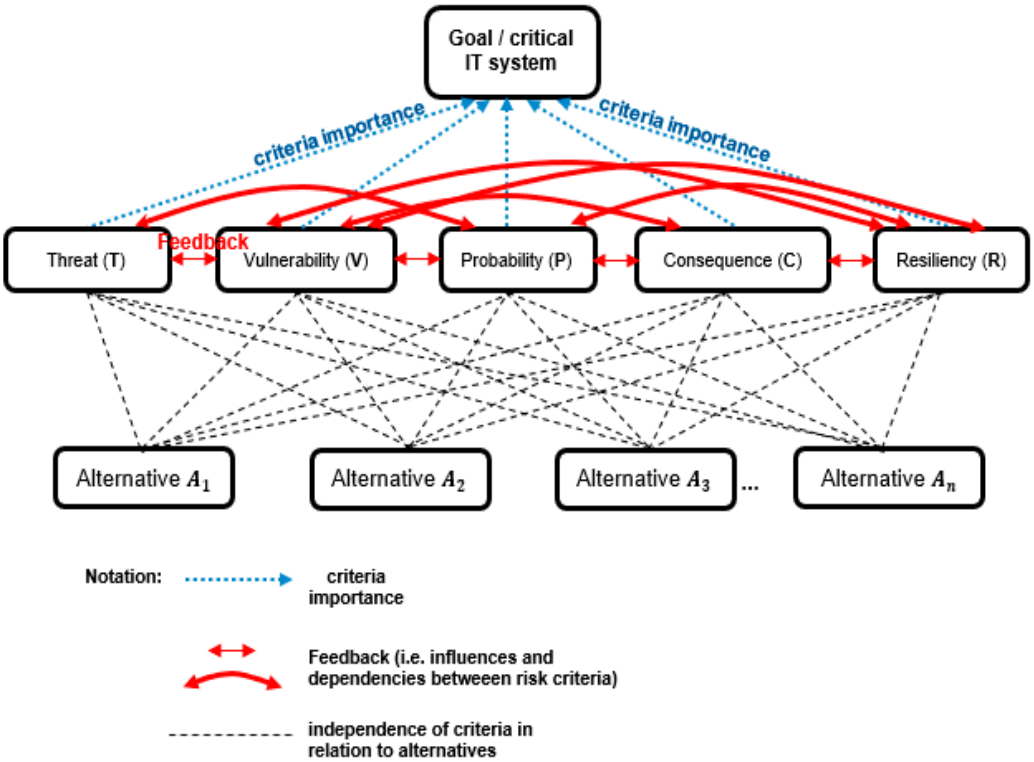

Figure 5. Multicriteria model with ISRA elements for the evaluation of critical IT systems.

On top of the hierarchy, there is a goal (asset) defined, i.e., decision on the best available IT solution among compared alternatives. In the middle, there are 5 generic ISRA elements that serve as evaluation criteria for the assessment of critical IT systems. Those 5 ISRA elements represent the core of the model and a novelty, i.e., scientific contribution in 2 important aspects: influences and dependencies (feedback) between ISRA elements are defined, and the importance of risk criteria in relation to the goal of decision-making is also taken into account.

Additionally, from Figure 5, it can be seen that evaluation criteria and alternatives (IT systems) are not dependent on each other (nor any arrow types defined). This means that the model is generic (as are its ISRA evaluation criteria) and applicable to the assessment of various IT solutions, not tailored to or dependent on a specific IT system.

By presenting a new multicriteria model in the demonstration research phase, according to the design science methodology, the defined research goal SG2 is successfully achieved, which enables the transition to the next research phase related to the validation of the model itself.

6. Model Validation—Case Study

The validation process is an extremely important step in the DSRM paradigm, in order to obtain information on whether the newly created artifact gives the expected (better) results compared to a reference model (if any). Validation of the multicriteria hybrid model was performed with the case study of a bank's online transaction systems. The aim of the case study was to examine the applicability and validity (H1) and effectiveness (H2) of the new multicriteria model with regard to critical IT systems in a financial institution, and to achieve the specific objective SG3.

This case study evaluated the most important banking transaction systems from the perspective of information security experts who work in the financial industry. Online systems are those systems available via the Internet to end users to perform transactions (e.g., electronic payments). The most important transaction systems identified by the number of active users and available via the Internet are the following: e-banking, m-banking, and e-commerce. In total, 16 information security experts from various European financial institutions and fintech companies participated in the model evaluation. Given that previous research had already defined the weights of generic ISRA criteria, it was necessary to establish the following five steps in the validation process for a case study of critical online banking transaction systems:

1. Defining the inherent criteria of critical online banking transaction systems
   As a basis for defining the inherent (common) criteria for critical banking transaction systems, the research from [64] was used where security objectives and security mechanisms were analyzed and defined. A security mechanism is defined as an established process by which certain security objectives are achieved. Thus, the inherent criteria for the case study of critical banking transaction systems were defined as follows: authentication, authorization, encryption, digital signing, availability, logging, and backup. IT security experts were in agreement on these criteria.
2. Defining the weights of the inherent criteria of banking transaction systems
   The research was performed in the same way as for the generic ISRA criteria in 2 subphases:
   Phase 1: Security experts provided their ratings on the DEMATEL scale for the impacts (dependencies) between the common criteria for transaction systems.
   Figure 6 shows the matrix (7×7) that was sent to IT security professionals for completion. It was the same as that in the case with ISRA criteria weights; after collecting the answers, aggregation of received values was performed and all other necessary computations were conducted according to the steps of the SNAP method [44]. The results of this step were the weights of the inherent criteria for online transaction systems corresponding to those obtained with the SNAPv12 method, which are shown in Table 5.
   However, because the SNAPv12 method does not take into account comparisons of criteria in relation to the decision goal, which is important due to the definition of the research problem, phase 2 was needed to calculate the final weights of common criteria of online banking transaction systems using the targeted SNAPv11 method.
   Phase 2: Security experts provided their ratios on the importance of defined inherent criteria for online transaction systems in relation to the goal of decision-making using the AHP. The identified inherent criteria for critical banking transaction systems were divided into a total of 3 clusters. The cluters were segmented according to the logical principle that is most suitable for defined transaction systems and research issues identified by a consensus of information security experts. The following clusters with their elements were defined: identity (authentication and authorization), C-I-A (encryption, digital signing, and availability) and forensics (logging and backup). Pairwise comparisons were made between the inherent criteria within each cluster and also between the three clusters defined by IT security experts that work in the financial sector.

Table 6 shows the inherent criteria weights obtained by input judgments from IT experts and the necessary calculations with the AHP. It is the same intermediate step that was performed when calculating the ISRA criteria weights. Again, in order to obtain the final inherent criteria weights, it was necessary to calculate arithmetic mean of the values obtained with the SNAPv12 method and the AHP intermediate step, as presented in Tables 5 and 6.

The final weights of the inherent criteria for banking online transaction systems obtained by the SNAP11 method were as follows:

It can be seen from Table 7 that there are no large discrepancies between the weights of the inherent criteria for transaction systems, and that this is in fact a normal distribution with the encryption criterion having the highest weight.

Additionally, as in the case with generic ISRA criteria, calculations of reference rankings for inherent criteria were performed using r_w and *WS* coefficients. Table 8 shows coefficients r_w and *WS* for inherent criteria for online banking transaction systems. Again, the *WS* coefficient seemed to be much more consistent and precise for measurements of the similarity of rankings for inherent criteria.

3. Evaluation of critical online transaction systems using inherent criteria
   Information security experts evaluated online banking transaction systems using the inherent criteria within the AHP method, and in doing so asked a general question: which transaction system is of better quality (and how much on the Saaty scale) in regards to the observed inherent criterion? For each transaction system, the implemented security controls in relation to the observed criterion should have been taken into account when making judgments. For example, when evaluating critical transaction systems according to the authentication criterion, information security experts should have taken into account the authentication factors implemented on each transaction system itself as well as the means for their implementation, e.g., username and password, biometrics, two-factor authentication, etc. Security experts also evaluated transaction systems according to all other defined inherent criteria. Finally, all judgments were aggregated (using a geometric mean) for each observed inherent criterion, and the eigenvectors of those inherent criteria were calculated for each transaction system, as listed in Table 9.
4. Evaluation of critical online transaction systems using generic ISRA criteria
   Information security experts evaluated banking transaction systems using the generic ISRA criteria within the AHP method, and in doing so asked a general question: which transaction system has a higher risk exposure compared to the observed risk criterion? For each observed ISRA criterion, the factors that may additionally affect the risk (according to the OWASP risk rating methodology [65]) of the banking transaction system in relation to the observed criterion also should have been taken into account. In other words, when evaluating critical transaction systems in relation to the threat criterion, it was necessary to consider which system is more exposed to different cyber security threats, e.g., malicious software, eavesdropping, hijacking, impersonating, unauthorized access, identity theft, DDoS attacks, more frequent ransom denial of service (RDoS) extortion attacks, etc. Security experts also evaluated transaction systems according to all other defined generic ISRA criteria. Finally, all judgments were aggregated (using geometric mean) for each observed ISRA criterion, and the eigenvectors of the ISRA criteria were calculated for each transaction system, as listed in Table 10.
5. Comparisons of the results obtained by inherent and generic criteria
   In order to confirm the H1 hypothesis in the validation process, it was necessary to perform a ranking and comparison of the results obtained by applying the hybrid multicriteria model in both cases, with the inherent and generic ISRA criteria, for banking transaction systems. Thus, when evaluating transaction systems according to the inherent and generic ISRA criteria, the following results were obtained, i.e., the

ranking of alternatives (the result of the multiplication of eigenvectors and SNAP11 criteria weights, as shown in Table 11):

Table 11 shows that mobile banking had the highest weight, which would mean that, according to information security experts, it is the online banking transaction system that has the best security mechanisms and controls in place compared to other observed systems. This was followed by e-banking and finally e-commerce with the lowest weight.

Table 12 shows that the e-commerce transaction system had the highest weight, followed by e-banking and finally m-banking with the lowest weight. However, it is important to note that when evaluating critical transaction systems according to ISRA criteria, it was necessary to apply the reverse logic for evaluation of the same systems using inherent criteria where it was determined which transaction system had implemented better security mechanisms or control. On the other hand, when evaluating transaction systems according to generic ISRA criteria, we assessed which system was actually more risky compared to the observed generic ISRA criterion. Thus, the results for evaluation according to ISRA criteria were interpreted in a way that reflected which transaction system was more risky (in the same way that judgments/ratios were given). Therefore, the ranking of alternatives (i.e., transaction systems) according to generic ISRA criteria was interpreted in such a way that the transaction system with the lowest weight was considered the least risky at the time of evaluation and thus actually took first place in the ranking. When such reverse logic is applied to the results obtained from evaluations of transaction systems using generic ISRA criteria, m-banking was the least risky system followed by e-banking while the most risky system was considered to be e-commerce. Therefore, the rank obtained by assessing transaction systems using inherent criteria corresponded to the rank obtained by evaluating the same systems using generic criteria for risk analysis and assessment. It follows that theH1 hypothesis was confirmed in a case study for critical online banking transaction systems.

Criteria influences for critical online transaction systems in the bank (m-banking, e-banking, e-commerce)	Auth	Atz	Enc	DS	Av	Log	Bck
Authentication (Auth)	0						
Authorization (Atz)		0					
Encryption (Enc)			0				
Digital signature (DS)				0			
Availability (Av)					0		
Logging (Log)						0	
Backup (Bck)							0

0 (no influence)
1 (low influence)
2 (medium influenc
3 (high influence)
4 (very high influer

Figure 6. Matrix for estimating influences and dependencies between inherent critera for transaction systems.

A simple full-time equivalent (FTE) metric was used to test the H2 hypothesis. In doing so, security experts recorded how much time they needed to complete the defined comparison tables when evaluating transaction systems with generic ISRA criteria in relation to the evaluation, i.e., validation of the model with inherent criteria. The measurement showed that security experts needed an average of 5.67 h to properly complete the tables for evaluation of transaction systems with inherent criteria, while the same respondents needed an average of 3.95 h to properly complete the tables when evaluating banking transaction systems with generic ISRA criteria. The measurements also included the time spent on additional assessments that were required due to errors made in the initial assessments

by some respondents, e.g., due to gaps in the table fields, inadequately set reciprocity, or inadequate calculations of the consistency index (CI) within the AHP method. Given that security experts realistically needed less time to evaluate transaction systems using the generic ISRA criteria than when evaluating transaction systems by inherent criteria, the H2 hypothesis regarding the effectiveness of a multicriteria model with generic criteria for risk analysis and assessment was confirmed.

Table 5. Weights of inherent criteria for transaction systems obtained by SNAP12.

Inherent Criteria for Transaction Systems (SNAP12)	Weight (SNAP12)
Authentication	0.135265454
Authorization	0.105908484
Encryption	0.173263665
Digital signature	0.117567661
Availability	0.241961344
Logging	0.099104201
Backup	0.126929191

Table 6. Weights of inherent criteria of transaction systems obtained by the AHP.

Inherent Criteria for Transaction Systems (AHP)	Weight (AHP)
Authentication	0.205736222
Authorization	0.164580753
Encryption	0.203349261
Digital signature	0.153751556
Availability	0.074480352
Logging	0.110567964
Backup	0.087533891

Table 7. Criteria weights of inherent elements for transaction systems obtained by SNAP11.

Inherent Criteria for Transaction Systems (SNAP11)	Weight (SNAP11)
Authentication	0.170500838
Authorization	0.135244618
Encryption	0.188306463
Digital signature	0.135659609
Availability	0.158220848
Logging	0.104836083
Backup	0.107231541

Table 8. Summary of reference rankings (R_x) for inherent criteria for transaction systems.

ISRA Criteria	SNAP12 Rank (R_x)	AHP Rank ($R_y^{(1)}$)	SNAP11 Rank ($R_y^{(2)}$)
Authentication	3	1	2
Authorization	6	3	5
Encryption	2	2	1
Digital signature	5	4	4
Availability	1	7	3
Logging	7	5	7
Backup	4	6	6
Coefficients	r_w	0.004464286	0.758928571
	WS	0.376041667	0.699479167

Table 9. Eigenvectors of inherent criteria for transaction systems.

Alternatives/Criteria	Auth	Atz	Enc	DS	Av	Log	Bck
e-banking	0.372191993	0.386198686	0.359962141	0.442262711	0.405931898	0.393551596	0.371068639
m-banking	0.426442961	0.388951499	0.410070356	0.388810918	0.378993865	0.388203063	0.384273720
e-commerce	0.201365046	0.224849816	0.229967503	0.168926371	0.215074237	0.218245341	0.244657641

Table 10. Eigenvectors of generic ISRA criteria for transaction systems.

Alternatives/Criteria	Threat (T)	Vulnerability (V)	Probability (P)	Consequence (C)	Resiliency (R)
e-banking	0.300439318	0.346069687	0.392030313	0.471548400	0.307823618
m-banking	0.312925954	0.250583450	0.244493668	0.319128828	0.312331238
e-commerce	0.386634729	0.403346863	0.363476020	0.209322771	0.379845144

Table 11. Rank of online transaction systems according to inherent criteria.

Transaction Systems (Inherent Criteria)	Rank/Weight
e-banking	0.388746283
m-banking	0.397145997
e-commerce	0.21410772

Table 12. Rank of transaction systems according to generic ISRA criteria.

Transaction Systems (Generic ISRA Criteria)	Rank/Weight
e-banking	0.350640726
m-banking	0.291067527
e-commerce	0.358291747

7. Discussion

The proposed model has several significant characteristics. First are the defined generic criteria for risk assessment and analysis that should facilitate the evaluation process for critical IT systems, where less resources (in terms of time and FTE) are required—no need for additional research on inherent criteria and calculations of their weights every time for different IT systems, as Figure 7 illustrates.

Figure 7 shows clearly that the process of evaluating IT systems is much shorter when generic ISRA criteria are used in comparisons than when inherent criteria are used. Thus, the proposed model with ISRA criteria is more efficient in comparison to the model with inherent criteria, as concrete numbers showed during the validation process.

The use of generic criteria for risk assessment can be viewed as a certain shortcoming of the model itself because inherent evaluation attributes will definitely always better fit their systems in comparison to certain generic evaluation criteria. However, we managed to confirm through a case study that the presented model gives the same results (rank of alternatives) as the model with inherent criteria for IT systems assessment. The most significant features of the model are the defined influences and dependencies (feedback) between the generic ISRA evaluation criteria. As already discovered in the systematic literature review [18], the feedback between evaluation elements is quite often neglected in many existing multicriteria models. One additional advantage of the model is the independence of the evaluation criteria in relation to alternatives. This implies universality of the model in that it should support the assessment of different IT systems, and not just certain very specific ones.

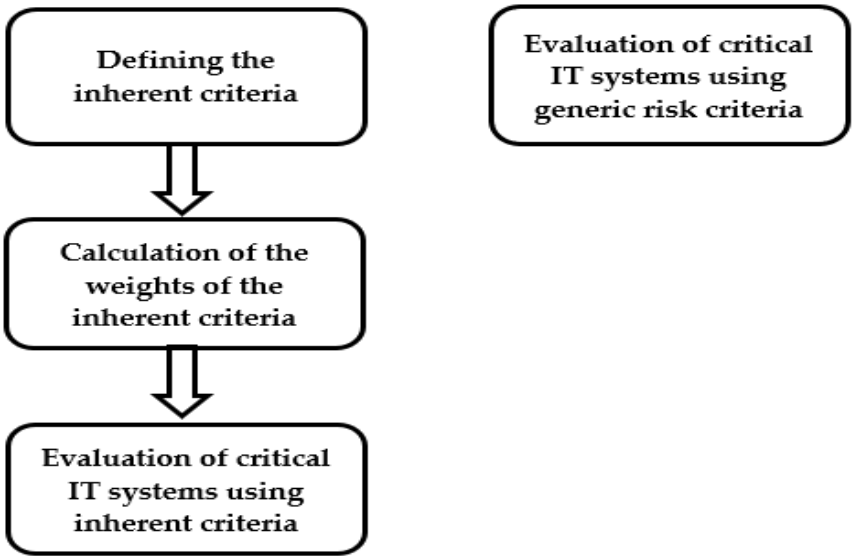

Figure 7. Evaluation steps.

In the model validation process, the applicability and efficiency of the model was demonstrated. The reason to choose the same methodology for both generic ISRA criteria and inherent criteria for the purposes of the definition, clustering, computation, and evaluation of alternatives is that some other referent models were not found during the SLR. Moreover, this approach seems to be the most precise in terms of assessing and ranking critical IT systems. The case study on critical online banking transaction systems showed that the model is valid because the ranking of alternatives was matched when the transaction systems were assessed using generic ISRA and inherent criteria.

The reasons why IT security professionals are convinced that the m-banking solution is the best in both cases, according to generic ISRA and inherent evaluation criteria, could be the following:

- Today's modern mobile banking applications are native versions, which means they are tailored to specific operating systems (i.e., iOS and Android) where rigorous tests must be performed before they can be released and made available for download through online app stores (especially Apple Store).
- Because m-banking apps are native, that means they are usually not prone to the most common web attacks, such as cross-site scripting (XSS) or SQL injections, because no common web components are included in them, unlike classic internet banking and especially e-commerce applications. Moreover, m-banking apps most often use strong (two-factor) authentication, where one authentication factor is the mobile device itself and the other one is a PIN or biometric element (fingerprint or face recognition). On the other hand, some e-commerce sites still even do not require strong authentication or additional elements for transaction authorization.
- Despite the enormous popularity of mobile apps, the main cyber-attacks today are still web related because attacking a web application requires less effort and knowledge in comparison to attacking a mobile app. However, that trend is certain to change in the future. Hence, the recommendation will be to definitely repeat the evaluation of online banking transaction systems within the next 2 years, possibly with a larger number of IT security experts involved.

In the future, we plan is to calibrate the existing multicriteria model for improved efficiency by eliminating the resiliency element (because it had the lowest agreement index in the Delphi research), cluster other ISRA criteria into two separate clusters, and then compare the results obtained from the case study on transaction systems. Additionally, for future research, we plan to pursue the fuzzification of input values for generic ISRA criteria in order to eventually decrease the impact of extreme ratios between the evaluation

criteria (e.g., 7:1 or 9:1 on the Saaty scale) given in some cases by IT security experts, and consequently to achieve even more precise results during the evaluation process for critical IT systems.

8. Conclusions

Due to the significant increase in security threats and vulnerabilities, and often the lack of time and resources to combat them efficiently in the business environment, prioritizing risks and addressing the most critical ones seems to be a fundamental problem. This is very important for critical elements of infrastructure such as financial institutions and their complex IT systems. The assessment and selection of an appropriate IT solution would also be a way to adequately manage information security risks.

Thus, we have proposed a new multicriteria model with a strong mathematical foundation for more efficient management of risks in terms of assessing and selecting critical information systems where the main advantage of the model is the use of generic attributes for risk analysis and assessment as evaluation criteria. The validity of the new multicriteria model was proven in the case study on online banking transaction systems. The presented model demonstrates another way to address cyber security risks by evaluating critical IT systems with generic ISRA criteria, where the obtained results should help decision-makers gain better insight into the security posture of their existing systems, or when new systems from different vendors need to be acquired or compared. The contribution from the new multicriteria model is particularly reflected in the fact that it takes into account the influences and dependencies (feedback) between the evaluation criteria. This is very important because the evaluation criteria are quite often dependent on and/or influence one another, a fact that has actually been neglected in other multicriteria models.

Future work will include tests of the model in other case studies to confirm its validity and effectiveness: e.g., through evaluations of critical server operating systems in financial institutions, comparisons of existing banking transaction systems with specific cryptosystems (e.g., Bitcoin), evaluations of selected cloud services, etc.

There are still many more open issues in the field of information security risk assessment and risk management. Hence, we are convinced that the application of MCDM in the information security risk management field will likely remain popular and show potentially significant growth in the coming years, specifically for the creation of new hybrid mathematical models.

Author Contributions: Conceptualization and methodology, D.M.; validation, I.M. and N.B.R.; writing—original draft preparation, D.M.; writing—review and editing, all authors; funding acquisition, I.M. and N.B.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported in part by the Croatian Science Foundation under the project IP-2019-04-4864.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All mathematical calculations along with the detailed procedures are available upon request.

Acknowledgments: We are very thankful to all the participants (i.e., information security experts) for their valuable feedback during all of the research phases.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

In this appendix we provide research questionnaires for both of the Delphi rounds.

Research question	Moderator's explanations	
Do you consider **Threat** (T) as a critical risk element necessary for evaluation of IT and IT security solutions?	**Threat** represents the probability of an event in which an attacker will make some damage to a particular business system. The analysis of threats is the first step that needs to be done in the process of risk assessment. Some of the most important threats in financial institutions are unauthorized access, malicious programs like viruses and worms, channel interception, data disclosure, denial of services that must be available 24x7 (e.g. online and mobile banking, e-commerce), etc.	
Do you consider **Vulnerability** (V) as a critical risk element necessary for evaluation of IT and IT security solutions?	**Vulnerability** is a characteristic of an IT asset or business process to indicate its weakness to some kind of attack. Vulnerability is linked to a **threat** that exploits it.	
Do you consider **Probability** (P) (or **Likelihood**) as a critical risk element necessary for evaluation of IT and IT security solutions?	According to **OWASP Risk Rating Methodology**, factors to assess the **Likelihood** are the following:	
	1. Threat agent factors: Skill level Participant Motive Method Opportunity Size Frequency of attack	2. Vulnerability factors: Ease of discovery Ease of exploit Awareness Intrusion detection
Do you consider **Consequence** (C) (or Impact) as a critical risk element necessary for evaluation of IT and IT security solutions?	**Consequence** represents a loss of economic, symbolic or psychological value for organization (i.e. reputational risk for the bank in case of loss or theft of data, unavailability of certain parts of information systems, reduced levels of service quality, etc.). According to **OWASP Risk Rating Methodology**, factors to assess the level of **Impact** are the following:	
	1. For technical impact: Loss of confidentiality Loss of integrity Loss of availability Loss of accountability	2. For business impact: Financial damage Reputation damage Non-compliance Privacy violation
Do you consider **Resiliency** (R) as a critical risk element necessary for evaluation of IT and IT security solutions?	The element is considered to evaluate how much and whether the IT solution is resilient regarding the other risk elements (**T**, **V**, **P**, **C**) that make influence on **Resiliency**. **Resilience** or **elasticity** is the speed with which the organization can successfully recover, reorganize itself and prepare to resume operations after a significant violation or failover of prescribed security policies. For the purpose of this research, resiliency attirbute is considered to be used for the evaluation of IT solutions.	
Do you consider any other critical risk element that should be included in the set of criteria for evaluation of IT and IT security solutions (**Yes**/**No**)?	If **Yes**, then the detailed rationale for additional risk element is **mandatory**. Feel free to write your suggestions.	

Figure A1. Research questionnaire for the first Delphi round. Five risk assessment attributes were presented for evaluation (closed questions), while one open question was included for IT security experts to consider any additional elements that could be part of the new hybrid multicriteria model.

Set of individual questions: **With these questions, the intention is to get more valuable info that makes You fully competent for giving necessary judgements related to Risk management topic in the research.**		**Answer (mandatory)**	**Moderator's explanations**
1	Please indicate your education degree.		case Your answer is **Other**, feel free to write some comments.
2	Please indicate all professional **certificates** you hold related to **information security**.	Bacc. Ing. Mag. PhD Other	g., CISSP, CISM, CEH, Security+, OSCP, GIAC, CRISC, etc. el free to write all.
3	Please indicate the **number** of years of Your **work experience** in the field of IT and **Information Security**.		e number of years of Your experience in **IT** and **IT Security area** required, not your overall work experience in other non-IT areas.
4	Do You hold managerial position in your organization at the moment?		E.g., CSO, CISO, CIO, BCM, Head of antifraud, etc.

Figure A2. Set of the individual questions for IT security experts necessary to obtain the level of competence of respondents in the domain of information security.

No.	Research question	Answer (mandatory)	Results of the first phase (just for Your orientation)			
			Mode		Arithmetic mean (average)	Standard deviation (SD)
			Value	Frequency		
1	Do you consider **Threat** (T) as a critical risk element necessary for evaluation of IT and IT security solutions?		5 - Strongly agreed	24 (out of 38)	4,55	0,6857
2	Do you consider **Vulnerability** (V) as a critical risk element necessary for evaluation of IT and IT security solutions?	1 - Strongly disagreed 2 - Disagreed 3 - Neutral 4 - Agreed 5 - Strongly agreed	Strongly agreed	23 (out of 38)	4,53	0,6872
3	Do you consider **Probability** (P) (or **Likelihood**) as a critical risk element necessary for evaluation of IT and IT security solutions?		5 - Strongly agreed	21 (out of 38)	4,34	0,8785
4	Do you consider **Consequence** (C) (or Impact) as a critical risk element necessary for evaluation of IT and IT security solutions?		5 - Strongly agreed	25 (out of 38)	4,63	0,5413
5	Do you consider **Resiliency** (R) as a critical risk element necessary for evaluation of IT and IT security solutions?		5 - Strongly agreed	16 (out of 38)	4,13	0,9056
6	Do you consider **Ease of Exploit** (E) as a critical risk element necessary for evaluation of IT and IT security solutions?		N/A	N/A	N/A	N/A

Figure A3. Research questionnaire for the second Delphi round, which presented statistics from the first Delphi round and also included an exploitability (E) element for rating as a potential additional criterion for the new multicriteria model.

Appendix B

SNAP11 procedure for calculating the weights of generic ISRA criteria.

Table A1. Aggregation of inputs received from IT security experts.

Aggregation (Z Matrix)	**(T)**	**(V)**	**(P)**	**(C)**	**(R)**
Threat (T)	**0**	2.4348	2.4783	2.6522	1.6522
Vulnerability (V)	3.0000	**0**	3.0435	2.6087	2.3478
Probability (P)	2.3043	1.6957	**0**	1.7391	1.5652
Consequence (C)	2.0435	1.6957	1.6522	**0**	2.3913
Resiliency (R)	1.9565	1.9565	1.6522	2.9565	**0**
Calculation of column sums and identification of max column sum	9.3043	7.7826	8.8261	9.9565	7.9565
Max column sum increased by 1, i.e.,: 1/(9.9565 + 1)				0.0913	

Table A2. Matrix calculations according to SNAP methodology.

S Matrix	**(T)**	**(V)**	**(P)**	**(C)**	**(R)**
Threat (T)	0	0.2222	0.2262	0.2421	0.1508
Vulnerability (V)	0.2738	0	0.2778	0.2381	0.2143
Probability (P)	0.2103	0.1548	0	0.1587	0.1429
Consequence (C)	0.1865	0.1548	0.1508	0	0.2183
Resiliency (R)	0.1786	0.1786	0.1508	0.2698	0
E matrix (n = 5)	(T)	(V)	(P)	(C)	(R)
Threat (T)	0.2	0.2	0.2	0.2	0.2
Vulnerability (V)	0.2	0.2	0.2	0.2	0.2
Probability (P)	0.2	0.2	0.2	0.2	0.2
Consequence (C)	0.2	0.2	0.2	0.2	0.2
Resiliency (R)	0.2	0.2	0.2	0.2	0.2
G matrix	(T)	(V)	(P)	(C)	(R)
Threat (T)	0.03	0.2189	0.2223	0.2358	0.1582
Vulnerability (V)	0.2627	0.03	0.2661	0.2324	0.2121
Probability (P)	0.2088	0.1615	0.03	0.1649	0.1514
Consequence (C)	0.1885	0.1615	0.1582	0.03	0.2155
Resiliency (R)	0.1818	0.1818	0.1582	0.2594	0.03
I − G	(T)	(V)	(P)	(C)	(R)
Threat (T)	1	−0.2189	−0.2223	−0.2358	−0.1582
Vulnerability (V)	−0.2627	1	−0.2661	−0.2324	−0.2121
Probability (P)	−0.2088	−0.1615	1	−0.1649	−0.1514
Consequence (C)	−0.1885	−0.1615	−0.1582	1	−0.2155
Resiliency (R)	−0.1818	−0.1818	−0.1582	−0.2594	1
Inverse (I − G)	(T)	(V)	(P)	(C)	(R)
Threat (T)	1.7076	0.8042	0.8631	0.9321	0.7723
Vulnerability (V)	1.0106	1.7086	0.9833	1.0291	0.8930
Probability (P)	0.7732	0.6708	1.5785	0.7723	0.6701
Consequence (C)	0.7842	0.6938	0.7387	1.6601	0.7409
Resiliency (R)	0.8198	0.7429	0.7769	0.9092	1.6009

Table A3. Multiplication of the matrix **G** by the inverse matrix $(I-G)^{-1}$.

G * Inverse (I − G)	(T)	(V)	(P)	(C)	(R)
Threat (T)	0.7588	0.8283	0.8890	0.9601	0.7955
Vulnerability (V)	1.0409	0.7599	1.0128	1.0600	0.9198
Probability (P)	0.7964	0.6910	0.6259	0.7955	0.6902
Consequence (C)	0.8077	0.7147	0.7609	0.7099	0.7631
Resiliency (R)	0.8444	0.7651	0.8002	0.9365	0.6489
Sum of columns	4.2483	3.7590	4.0888	4.4619	3.8175

Table A4. Detailed calculations of SNAP11 criteria weights.

	r	c	r − c	N1	SNAP12	AHP	SNAP11
Threat (T)	4.2317	4.2483	−0.0166	1.7235	0.1981	0.1058	0.151960196
Vulnerability (V)	4.7934	3.7590	1.0344	2.7744	0.3189	0.1868	0.252842812
Probability (P)	3.5989	4.0888	−0.4899	1.2502	0.1437	0.0572	0.100434911
Consequence (C)	3.7562	4.4619	−0.7057	1.0344	0.1189	0.1964	0.157652935
Resiliency (R)	3.9952	3.8175	0.1778	1.9179	0.2204	0.4538	0.337109146

References

1. Wheeler, E. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*; Elsevier Inc.: Waltham, MA, USA, 2011.
2. Von Roessing, R. The ISACA Business Model for Information Security: An Integrative and Innovative Approach. In *ISSE 2009 Securing Electronic Business Processes*; Vieweg+Teubner: Wiesbaden, Germany, 2010; pp. 37–47.
3. Mohyeddin, M.A.; Gharaee, H. FAHP-TOPSIS Risks Ranking Models in ISMS. In Proceedings of the 7th International Symposium on Telecommunications (IST), Tehran, Iran, 9–11 September 2014; pp. 879–881.
4. Raghavan, A.R.; Parthiban, L. The effect of cybercrime on a Bank's finances. *Int. J. Curr. Res. Acad. Rev.* **2014**, *2*, 173–178.
5. Biancotti, C. Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys. *Bank Italy Occas. Pap.* **2017**, *373*. [CrossRef]
6. Bouveret, A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Work. Pap. Int. Monet. Fund.* **2018**, *18*.
7. Aidan, J.S.; Verma, H.K.; Awasthi, L.K. Comprehensive Survey on Petya Ransomware Attack. In Proceedings of the International Conference on Next Generation Computing and Information Sciences (ICNGCIS), Jammu, India, 11–12 December 2017; pp. 122–125.
8. Hsiao, S.-C.; Kao, D.-Y. The Static Analysis of WannaCry Ransomware. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 153–158.
9. Verizon Enterprise. Data Breach Investigations Report, Public Sector Excerpt. 2020. Available online: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (accessed on 5 April 2021).
10. Lagarde, C. Estimating Cyber Risk for the Financial Sector. IMFBlog, Insights & Analysis on Economics & Finance. 2018. Available online: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/ (accessed on 5 April 2021).
11. Interpol. INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19. Available online: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed on 5 April 2021).
12. Hakak, S.; Khan, W.Z.; Imran, M.; Choo, K.-K.R.; Shoaib, M. Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access* **2020**, *8*, 124134–124144. [CrossRef]
13. NIST. SP 800-30: Guide for Conducting Risk Assessments, Joint Task Force Transformation Initiative, Revision 1. 2012. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 5 April 2021).
14. NIST. SP 800-37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Joint Task Force, Revision 2. 2018. Available online: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final (accessed on 5 April 2021).
15. Mbowe, J.E.; Zlotnikova, I.; Msanjila, S.S.; Oreku, G.S. A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. *J. Inf. Secur.* **2014**, *5*, 166–177. [CrossRef]
16. Maček, D.; Magdalenić, I.; Begičević Ređep, N. Towards a Hybrid Model for the Evaluation of Critical IT Systems. In Proceedings of the 31st Central European Conference on Information and Intelligent Systems (CECIIS), Varaždin, Croatia, 7–9 October 2020; Faculty of Organization and Informatics Varaždin, University of Zagreb: Varaždin, Croatia, 2020; pp. 249–255.
17. Kitchenham, B. Guidelines for performing Systematic Literature Reviews in Software Engineering. In *EBSE Technical Report*; Software Engineering Group, School of Computer Science and Mathematics, Keele University: Keele, UK; Department of Computer Science, University of Durham: Durham, UK, 2007.

18. Maček, D.; Magdalenić, I.; Begičević Redep, N. A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment. *Int. J. Saf. Secur. Eng.* **2020**, *10*, 161–174.
19. Shameli-Sendi, A.; Aghababaei-Barzegar, R.; Cheriet, M. Taxonomy of information security risk assessment (ISRA). *Comput. Secur.* **2016**, *57*, 14–30. [CrossRef]
20. Pan, L.; Tomlinson, A. A systematic review of information security risk assessment. *Int. J. Saf. Secur. Eng.* **2016**, *6*, 270–281. [CrossRef]
21. Wangen, G.; Hallstensen, C.; Snekkenes, E. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* **2018**, *17*, 681–699. [CrossRef]
22. Alcántara, M.; Melgar, A. Risk management in information security: A systematic review. *J. Adv. Inf. Technol.* **2016**, *7*, 1–7. [CrossRef]
23. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98. [CrossRef]
24. Sumrit, D.; Anuntavoranich, P. Using DEMATEL method to analyze the causal relations on technological innovation capability evaluation factors in Thai technology-based firms. *Int. Trans. J. Eng. Manag. Appl. Sci. Technol.* **2013**, *4*, 81–103.
25. Saaty, T.L. *Decision Making with Dependence and Feedback: The Analytic Network Process: The Organization and Prioritization of Complexity*; RWS Publications: New York, NY, USA, 2001.
26. Saaty, T.L. Decision Making–The Analytic Hierarchy and Network Processes (AHP/ANP). *J. Syst. Sci. Syst. Eng.* **2004**, *13*, 1–35. [CrossRef]
27. Lo, C.-C.; Chen, W.-J. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Syst. Appl.* **2012**, *39*, 247–257. [CrossRef]
28. Yang, Y.-P.; Shieh, H.-M.; Tzeng, G.-H. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Inf. Sci.* **2013**, *232*, 482–500. [CrossRef]
29. Wu, T.; Zhao, G. A novel risk assessment model for privacy security in internet of things. *Wuhan Univ. J. Nat. Sci.* **2014**, *19*, 398–404. [CrossRef]
30. Zhang, K.; Shao, L. Research on the quantitative methods of classified information system security risk assessment. In Proceedings of the International Conference on Logistics, Informatics and Service Science (LISS), Berkeley, CA, USA, 25–28 July 2014; Springer: Berlin/Heidelberg, Germany, 2015; pp. 571–575.
31. Tianshui, W.; Gang, Z. A new security and privacy risk assessment model for information system considering influence relation of risk elements. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications (BECCA), Guangdong, China, 8–10 November 2014; pp. 233–238.
32. Hiete, M.; Merz, M.; Comes, T.; Schultmann, F. Trapezoidal fuzzy DEMATEL method to analyze and correct for relations between variables in a composite indicator for disaster resilience. *OR Spectrum* **2012**, *34*, 971–995. [CrossRef]
33. Kim, K.-Y.; Na, K.-S. Business information system recovery priority decision using TOPSIS on interval data. *J. Syst. Inf. Technol.* **2014**, *16*, 103–112. [CrossRef]
34. Tsai, H.-Y.; Huang, Y.-L. An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks. *IEEE Trans. Reliab.* **2012**, *60*, 801–816. [CrossRef]
35. Huang, Y.-L.; Sun, W.-L. An AHP-based risk assessment for an industrial IoT cloud. In Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 637–638.
36. Sałabun, W.; Wątróbski, J.; Shekhovtsov, A. Are MCDA Methods Benchmarkable? A Comparative Study of TOPSIS, VIKOR, COPRAS, and PROMETHEE II Methods. *Symmetry* **2020**, *12*, 1549. [CrossRef]
37. Rehman, A.u.; Shekhovtsov, A.; Rehman, N.; Faizi, S.; Sałabun, W. On the Analytic Hierarchy Process Structure in Group Decision-Making Using Incomplete Fuzzy Information with Applications. *Symmetry* **2021**, *13*, 609. [CrossRef]
38. Lo, H.-W.; Hsu, C.-C.; Huang, C.-N.; Liou, J.J.H. An ITARA-TOPSIS Based Integrated Assessment Model to Identify Potential Product and System Risks. *Mathematics* **2021**, *9*, 239. [CrossRef]
39. Michnik, J. Weighted Influence Non-linear Gauge System (WINGS)–An analysis method for the systems of interrelated components. *Eur. J. Oper. Res.* **2013**, *228*, 536–544. [CrossRef]
40. Ju, Y.; Wang, A.; You, T. Emergency alternative evaluation and selection based on ANP, DEMATEL, and TL-TOPSIS. *Nat. Hazards* **2015**, *75*, 347–379. [CrossRef]
41. Si, S.-L.; You, X.-Y.; Liu, H.-C.; Zhang, P. DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications. *Math. Probl. Eng.* **2018**. [CrossRef]
42. Kadoić, N.; Divjak, B.; Begičević Redep, N. Integrating the DEMATEL with the analytic network process for effective decision-making. *Cent. Eur. J. Oper. Res.* **2019**, *27*, 653–678. [CrossRef]
43. Fan, C.K.; Chen, T.-C. The risk management strategy of applying cloud computing. *Int. J. Adv. Comput. Sci. Appl.* **2012**, *3*, 18–27.
44. Kadoić, N.; Begičević Redep, N.; Divjak, B. A new method for strategic decision-making in higher education. *Cent. Eur. J. Oper. Res.* **2018**, *26*, 611–628. [CrossRef]
45. Henni, K.; Mezghani, N.; Gouin-Valleranda, C. Unsupervised graph-based feature selection via subspace and PageRank centrality. *Expert Syst. Appl.* **2018**, *114*, 46–53. [CrossRef]
46. Hashemi, A.; Bagher Dowlatshahi, M.; Nezamabadi-pour, H. MGFS: A multi-label graph-based feature selection algorithm via PageRank centrality. *Expert Syst. Appl.* **2020**, *142*. [CrossRef]

47. Roy, B. *Multicriteria Methodology for Decision Aiding (Nonconvex Optimization and Its Applications)*; Kluwer Academic Publishers: Dordrecht, The Netherlands, 1996.
48. Kornyshova, E.; Salinesi, C. MCDM Techniques Selection Approaches: State of the Art. In Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Multicriteria Decision Making, Honolulu, HI, USA, 1–5 April 2007; pp. 22–29.
49. Ishizaka, A.; Nemery, P. *Multi-criteria Decision Analysis: Methods and Software*, 1st ed.; John Wiley & Sons Ltd: West Sussex, UK, 2013.
50. Li, Y.; Thomas, M.A. A Multiple Criteria Decision Analysis (MCDA) software selection framework. In Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, USA, 6–9 January 2014; pp. 1084–1094.
51. Salinesi, C.; Kornyshova, E. Choosing a Prioritization Method—Case of IS Security Improvement. In Proceedings of the 18th Conference on Advanced Information Systems Engineering (CAiSE' 06), Forum Proceedings, Theme: Trusted Information Systems, Luxembourg, 5–9 June 2006.
52. Wątróbski, J.; Jankowski, J.; Ziebma, P.; Karczmarczyk, A.; Zioło, M. Generalised framework for multi-criteria method selection. *Omega* **2018**, *86*, 107–124. [CrossRef]
53. Wątróbski, J.; Jankowski, J.; Ziemba, P.; Karczmarczyk, A.; Zioło, M. MCDA Method Selection Tool. 2019. Available online: http://www.mcda.it/ (accessed on 5 April 2021).
54. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–78. [CrossRef]
55. Vaishnavi, V.; Kuechler, B. Design Science Research in Information Systems. Design Science Research in Information Systems and Technology. 2015. Available online: http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf/ (accessed on 5 April 2021).
56. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
57. Hevner, A.R. A Three Cycle View of Design Science Research. *Scand. J. Inf. Syst.* **2007**, *19*, 87–92.
58. Menold, N.; Bogner, K. *Design of Rating Scales in Questionnaires, GESIS Survey Guidelines, Version 2.0*; GESIS–Leibniz-Institut für Solzialwissenschaften: Mannheim, Germany, 2016.
59. Giannarou, L.; Zervas, E. Using Delphi technique to build consensus in practice. *Int. J. Bus. Sci. Appl. Manag.* **2014**, *9*, 65–82.
60. Brin, S.; Page, L. The Anatomy of a Large-Scale Hypertextual Web Search Engine. *7th International World-Wide Web Conference (WWW 1998).* Available online: http://infolab.stanford.edu/~{}backrub/google.html (accessed on 5 April 2021).
61. Sałabun, W.; Urbaniak, K. A New Coefficient of Rankings Similarity in Decision-Making Problems. In Proceedings of the International Conference on Computational Science (ICCS 2020), Amsterdam, The Netherlands, 3–5 June 2020; pp. 632–645.
62. Saaty, T.L. *Multicriteria Decision Making: The Analytic Hierarchy Process*; RWS Publications: Pittsburgh, PA, USA, 1980.
63. Bayazit, O. Use of AHP in decision-making for flexible manufacturing systems. *J. Manuf. Technol. Manag.* **2005**, *16*, 808–819. [CrossRef]
64. Cherdantseva, Y.; Hilton, J. *Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals. Organizational, Legal, and Technological Dimensions of Information System Administration (Chapter 10)*; IGI Global: Hershey, PA, USA, 2014.
65. OWASP Risk Rating Methodology, Category: OWASP Testing Project. 2019. Available online: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (accessed on 5 April 2021).