Complex & Intelligent Systems (2019) 5:113–126
https://doi.org/10.1007/s40747-018-0087-7

ORIGINAL ARTICLE

AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis

M. Fatih Ak[1] · Muhammet Gul[2]

Received: 6 September 2018 / Accepted: 3 December 2018 / Published online: 27 December 2018

Abstract

Risk analysis (RA) contains several methodologies that object to ensure the protection and safety of occupational stakeholders. Multi attribute decision-making (MADM) is one of the most important RA methodologies that is applied to several areas from manufacturing to information technology. With the widespread use of computer networks and the Internet, information security has become very important. Information security is vital as institutions are mostly dependent on information, technology, and systems. This requires a comprehensive and effective implementation of information security RA. Analytic hierarchy process (AHP) and technique for order preference by similarity to ideal solution (TOPSIS) are commonly used MADM methods and recently used for RA. In this study, a new RA methodology is proposed based on AHP–TOPSIS integration extended with Pythagorean fuzzy sets. AHP strengthened by interval-valued Pythagorean fuzzy numbers is used to weigh risk parameters with expert judgment. Then, TOPSIS with Pythagorean fuzzy numbers is used to prioritize previously identified risks. A comparison of the proposed approach with three approaches (classical RA method, Pythagorean fuzzy VIKOR and Pythagorean fuzzy MOORA) is also provided. To illustrate the feasibility and practicality of the proposed approach, a case study for information security RA in corrugated cardboard sector is executed.

Keywords Risk analysis · Information security · Multi attribute decision-making · Pythagorean fuzzy sets · AHP · TOPSIS · Corrugated cardboard sector

Introduction

Information is a tool that people use to communicate among themselves from the moment they start living together. The nature and type of information technology have changed dramatically over the past decade. Simple and single batch applications are transformed into distributed computing environments including multitasking real-time control, and distributed processing. It is at least as important as the information itself to determine that information is valuable or worthless, or to measure the value carried by it. The most general definition of information security is that our own information is not passed on to anyone else. It is a combination of three main elements called "privacy", "integrity", and "accessibility". Information is protected from unauthorized access which is called privacy. Integrity defined as information that is not altered by unauthorized persons. Information is available when authorized people are needed. Information is reachable and available when authorized people are needed which is called accessibility. If any of these three basic security elements are damaged, a security weakness occurs. Information security RA is essential for any corporate organizational system. It is essential to ensure that controls and expenditures are in full compliance with the risks that the organization is experiencing or experienced before. Organizations' heavy dependence on information systems necessitates managing risks related to them [1]. One of the most important aspects of information security is technical measures. Given better access control policy models, better tools for system assessment and assurance should be resolved, including better ways to detect cryptographic formal evidence, protocols, approved firewalls, intrusions and malicious codes [2].

✉ Muhammet Gul
muhammetgul@munzur.edu.tr

M. Fatih Ak
fatih.ak@antalya.edu.tr

[1] Department of Industrial Engineering, Antalya Bilim University, Antalya, Turkey

[2] Department of Industrial Engineering, Munzur University, 62000 Tunceli, Turkey

Information security RA is a dynamic process such that there is a requirement to be developed to discover, correct and for prevention of security problems. RA is a core part of a risk management process designed to set up required appropriate level of security for information systems [3]. The RA revealed a number of potential threats to the information security. Although technology is a kind of key element of information security, it does not consists of it alone. Information security RA has been influenced by variables such as new legal requirements [4]. Information security risk assessments are part of sound security practices. Today, with the widespread use of the internet and the development of technology, threats related to information security are increasing and diversifying. As a result, there is a rapid development of information security risk assessment ways. To ensure the security of computers and networks, to keep unauthorized persons away from the system, or to prevent them from entering the system and acquiring the information, firstly, comprehensive risk assessment is required for the whole system. RA is required at the point of information security. RA is an important component of compiling an information security policy for an organization. In addition, RA deals with all aspects of information security [5].

Managing information security is primarily a risk. Risk management usually involves performing a RA. Identifying and evaluating risks reduces the risks with using risk management techniques. Likewise, the standard approach to managing information security involves conducting a RA to identify the risks of privacy, integrity and availability.

Information systems are monitored by risk management. Control measures are used to mitigate these risks. The protection of information resources from the complicated and swiftly changing landscape of security threats is one of the most significant challenge for modern organization risk management. The main concern for any organization is the infiltration and alteration of sensitive information [6, 7].

Multi attribute decision-making (MADM) is an important methodology that a generic risk management standard—IEC 31010:2009—has mentioned on the selection and application of systematic techniques for RA. AHP and TOPSIS methods are most widely used MADM methods that come up with advantages of computational simplicity in different areas of research, the flexibility to integrate with other techniques and being independent of limitations. Since information security RA has challenging issues and conflicting parameters, AHP–TOPSIS-integrated method can supply advantages which are mentioned above. On the other hand, one of the significant expected contributions of integrating Pythagorean fuzzy sets in information security RA is the power to express uncertainty and depict the fuzziness which strengthened the proposed AHP–TOPSIS integration for information security RA model.

This paper aims to make information security RA comprehensive, efficient and effective with MADM methods by the integration of fuzzy logic. Pythagorean fuzzy sets-based model helps to minimize of uncertainties and improve the functionality of RA. Pythagorean fuzzy sets allows the user to determine uncertainties in the real world better and more accurately while helps to eliminate the uncertainties [8–12]. Application of Pythagorean fuzzy-based information security RA method can be applied to any information-based system to make them more functional.

The rest of this paper structured as follows: "Literature review" presents literature review, contribution to this study and research gaps on information security RA. "Methodology" presents methodology and method. In "Case study: information security RA for corrugated cardboard sector", the applications of case study, comparison, and discussion of result are presented. In the last section, concluding remarks and future recommendations are given.

Literature review

There are many quantitative, qualitative, knowledge-based, model-based risk assessment tools to analyze main reasons of risks in various industries and features of the companies. Quantitative RA methods use statistical and mathematical ways to represent risk while qualitative RA methods are analyzed by adjectives instead of them. Information systems security (ISS) checklist, standards, maturity criteria methods are classical RA methods. There are solutions and procedures and it is assumption when selected ISS checklists and procedures can be observed and converted into a list. Capturing the best practice and putting standards are targets of ISS standards for common, authoritative, and international use. Offering an objective and appropriate scale for classification is target of ISS maturity method.

MADM-based method is one of the most important and effective methods for RA of systems [13–22]. There are finite number of choices or alternatives existing and evaluated based on finite number of attributes or objectives. In these methods, decision makers often have difficulty in accurate rating and assessment throughout risk parameters. Therefore, implementing potential RA methods can show satisfactory results in terms of incomplete risk data or high uncertainty. Quantitative and qualitative techniques have some weak aspects and their own disadvantages in the RA process. While quantitative techniques have high level of uncertainty, qualitative techniques rely more on judgment than on statistical calculations while fuzzy sets make analysis more appropriate with respect to uncertainty, unpredictability, and effectiveness. Besides, fuzzy sets can increase testing accuracy of RA due to logic behind it. Information has numerical- and linguistic-type uncertainties. With the combination of fuzzy sets to information security RA process, identifying potential risk factors, evaluating the corresponding control measures can be done more detailed due to structure of fuzzy logic [23, 24]. In this case the ways that combining MADM and fuzzy sets are accepted to model the structure [25]. One of the important advantages of fuzzy MADM methods is relatively assessing the risk parameters using fuzzy numbers instead of crisp numbers. This is one of the significant advantages for the decision maker.

Various RA studies have been carried out in the field of information security [3, 4, 6, 7, 26, 27]. Today, information systems have a complex, intricate structure and common use. For this reason, detailed mathematical measures used to model for complex risk environments make the process more convenient. Process of RA is also quite complicated. Although mathematical and classical RA models are used in information security, these methods are not succeeded to cover whole information security process and risks related to it. It can be observed that previous studies on RA of information security are reactive and aim to prevent repetition of a fault while our proposed methodology is proactive and aim to prevent any event that has potential cause for loss by eliminating factors before fault occurs. In this study proposed method for information security RA also supplies opportunity to decrease uncertainty in system with comprehensive and detailed analysis of system by the aid of fuzzy set theory. This approach makes this study different from the previous studies.

On the other hand, several approaches are proposed regarding combination of fuzzy set theory and MADM methods recently. Table 1 shows some recent studies with different type of fuzzy sets applied, MADM method and characteristic of RA problem. According to the Table 2, AHP–TOPSIS integration is studied in Gul and Ak [28] and Carpitella et al. [29]. However, in both studies, trapezoidal fuzzy set-based TOPSIS was applied to prioritize hazards. In the first study, PFAHP was used in weighing two fundamental risk parameters named severity and probability. Then, hazards were prioritized using trapezoidal fuzzy number-based TOPSIS. In the second study, both methods were integrated with trapezoidal fuzzy numbers.

In the light of above-mentioned studies, it is easily seen that current study has contributions to the knowledge from both application view point (providing RA studies in the information security area) and methodological view point (providing Table 1 to show the recent RA studies by MADM methods and different versions of fuzzy set theory). (1) A novel integrated RA approach under Pythagorean fuzzy envi-

Table 1 Recent fuzzy MADM-based RA studies

Study	Version of fuzzy set	Applied MCDA method	Application area	Additional traditional RA method used
Gul and Ak [28]	Pythagorean fuzzy set	AHP, TOPSIS	Mining	5 × 5 risk matrix
Gul [31]	Pythagorean fuzzy set	AHP, VIKOR	Manufacturing	–
Oz et al. [21]	Pythagorean fuzzy set	TOPSIS	Pipeline construction	2-Dimensional risk matrix
Karasan et al. [33]	Pythagorean fuzzy set	AHP	Construction	FMEA, Fine–Kinney
Ilbahar et al. [32]	Pythagorean fuzzy set	AHP	Construction	FMEA, Fine–Kinney
Carpitella et al. [29]	Trapezoidal fuzzy set	AHP, TOPSIS	Environment	FMECA
Gul et al. [18]	Trapezoidal fuzzy set	AHP, VIKOR	Manufacturing	Fine–Kinney
Gul et al. [42]	Triangular fuzzy set and Pythagorean fuzzy set	AHP	Transportation	–
Fattahi and Khalilzadeh [50]	Triangular fuzzy set	AHP, MULTIMOORA	Manufacturing	FMEA
Wang et al. [43]	Triangular fuzzy set	Choquet integral	Transportation	FMEA
Wang et al. [44]	Triangular fuzzy set	Choquet integral, MULTIMOORA	Marine	Fine–Kinney
Can and Toktas [45]	Triangular fuzzy set	DEMATEL, MABAC	Manufacturing	Fine–Kinney
Can [46]	Intuitionistic fuzzy set	WASPAS	Manufacturing	FMEA
Gul et al. [13]	Triangular fuzzy set	AHP, VIKOR	Healthcare	–
Gul et al. [14]	Triangular fuzzy set	AHP, VIKOR	Marine	Fine–Kinney
Ozdemir et al. [22]	Interval type-2 fuzzy set	AHP, VIKOR	Education	FMEA
Yazdi [47]	Triangular fuzzy set	AHP	Chemistry	HAZOP, FTA
Yazdi and Kabir [48]	Fuzzy possibility score	AHP	Chemistry	FTA, Bayesian Network
Current study	Pythagorean fuzzy set	AHP, TOPSIS	Information security	–

Table 2 Difference between FTOPSIS, IFTOPSIS, and PFTOPSIS

Method	Definition	Advantages
FTOPSIS	A MCDM technique based on the concept of choosing the solution with the shortest distance from the ideal solution and the farthest distance from the negative ideal solution by considering concept of fuzzy sets	It has more capability in handling uncertainties, simultaneous consideration of the positive and the negative ideal points, simple computation, and logical concept
IFTOPSIS	A MCDM technique based on the concept of choosing the solution with the shortest distance from the ideal solution and the farthest distance from the negative ideal solution by considering concept of fuzzy sets whose elements have degrees of membership and non-membership	It uses a special case of the membership and non-membership functions considering the positive and the negative ideal points. Handling vagueness and uncertainty is over FTOPSIS because it considers three different grades of membership degree, hesitancy degree and non-membership degree
PFTOPSIS	A MCDM technique based on the concept of choosing the solution with the shortest distance from the ideal solution and the farthest distance from the negative ideal solution by considering concept of fuzzy sets whose elements have degrees of membership, non-membership and description of the sum of the degree is bigger than 1, but their square sum is equal to or less than 1	It has a membership grade which is greater than the space of the membership grade of intuitionistic FTOPSIS

ronment is provided. A PFAHP–PFTOPSIS integration in RA field has not been studied in the literature yet. (2) The integrated approach is tested in a real case study for information security RA in corrugated cardboard sector. (3) A comparative analysis with classical RA method that the observed facility followed is provided. (4) A new risk parameter called value of information, that is specific for information security, is considered in this study for the first time. The parameter of value of information refers to the sum of three factors as privacy, integrity, and accessibility.

Methodology

Pythagorean fuzzy sets and related notations

In this section, firstly, some preliminaries of Pythagorean fuzzy sets and corresponding notations are described. Then, the algorithm of Pythagorean fuzzy analytic hierarchy process (PFAHP) and Pythagorean fuzzy technique for order preference by similarity to ideal solution (PFTOPSIS) methods are explained with details. Pythagorean fuzzy sets were first proposed by Yager [30] and have been applied to various problems respecting uncertainty like interval type-2 fuzzy sets, hesitant fuzzy sets and intuitionistic fuzzy sets. Both intuitionistic fuzzy sets and Pythagorean fuzzy sets can be expressed in terms of membership function, non-membership function and hesitancy degree. However, in some cases, the degrees of membership and non-membership are bigger than 1 for intuitionistic fuzzy sets. To overcome the challenge, Yager [30] developed Pythagorean fuzzy sets. These sets are the generalization to the intuitionistic fuzzy sets in some condition where intuitionistic fuzzy sets cannot address the uncertainty. Therefore, Pythagorean fuzzy sets are more powerful and flexible to solve problems involving uncertainty [28, 31–34].

In Pythagorean fuzzy sets, the sum of membership and non-membership degrees can exceed 1 but the sum of squares cannot [8–12, 28, 31–33, 35, 36]. This situation is shown below in Definition 1.

Definition 1 Let a set X be a universe of discourse. A Pythagorean fuzzy set P is an object having the form [8, 9, 36–38]:

$$P = \{\langle x,\ P(\mu_{\mathrm{P}}(x), \upsilon_{\mathrm{P}}(x))\rangle | x \in X\}, \tag{1}$$

where $\mu_P(x) : X \mapsto [0, 1]$ defines the degree of membership and $\upsilon_{\mathrm{P}}(x) : X \mapsto [0, 1]$ defines the degree of non-membership of the element $x \in X$ to P, respectively, and, for every $x \in X$, it holds:

$$0 \le \mu_{\mathrm{P}}(x)^2 + \upsilon_{\mathrm{P}}(x)^2 \le 1. \tag{2}$$

For any PFS P and $x \in X$, $\pi_{\mathrm{P}}(x) = \sqrt{1 - \mu_{\mathrm{P}}^2(x) - \upsilon_{\mathrm{P}}^2(x)}$ is called the degree of indeterminacy of x to P.

Definition 2 Let $\beta_1 = P(\mu_{\beta_1}, v_{\beta_1})$ and $\beta_2 = P(\mu_{\beta_2}, v_{\beta_2})$ be two Pythagorean fuzzy numbers, and λ >0, then the operations on these two Pythagorean fuzzy numbers are defined as follows [35, 36]:

$$\beta_1 \oplus \beta_2 = P(\sqrt{\mu_{\beta_1}^2 + \mu_{\beta_2}^2 - \mu_{\beta_1}^2 \mu_{\beta_2}^2},\ v_{\beta_1} v_{\beta_2}) \tag{3}$$

$$\beta_1 \otimes \beta_2 = P\left(\mu_{\beta_1}\mu_{\beta_2},\ \sqrt{v_{\beta_1}^2 + v_{\beta_2}^2 - v_{\beta_1}^2 v_{\beta_2}^2}\right), \tag{4}$$

$$\lambda\beta_1 = P\left(\sqrt{1-(1-\mu_{\beta_1}^2)^\lambda}, (v_{\beta_1})^\lambda\right), \quad \lambda > 0, \tag{5}$$

$$\beta_1^\lambda = P\left((\mu_{\beta_1})^\lambda, \sqrt{1-(1-v_{\beta_1}^2)^\lambda}\right), \quad \lambda > 0. \tag{6}$$

Definition 3 Let $\beta_1 = P(\mu_{\beta_1}, v_{\beta_1})$ and $\beta_2 = P(\mu_{\beta_2}, v_{\beta_2})$ be two Pythagorean fuzzy numbers, a nature quasi-ordering on the Pythagorean fuzzy numbers is defined as follows [8–12, 36, 39, 40]:

$\beta_1 \geq \beta_2$ if and only if $\mu_{\beta_1} \geq \mu_{\beta_2}$ and $v_{\beta_1} \leq v_{\beta_2}$.

To compare magnitude of two Pythagorean fuzzy numbers, a score function is developed by Garg [8–12, 36, 39, 40] as follows:

$$s(\beta_1) = (\mu_{\beta_1})^2 - (v_{\beta_1})^2. \tag{7}$$

Definition 4 Depending on the proposed score functions of Pythagorean fuzzy numbers as demonstrated above, the following laws are defined to compare two Pythagorean fuzzy numbers [8–12, 36, 38, 39]:

(i) If $s(\beta_1) < s(\beta_2)$, then $\beta_1 \prec \beta_2$,
(ii) If $s(\beta_1) > s(\beta_2)$, then $\beta_1 \succ \beta_2$,
(iii) If $s(\beta_1) = s(\beta_2)$, then $\beta_1 \sim \beta_2$.

Proposed integrated approach

This section describes the theoretical background of the methods used in the proposed integrated approach. In the first sub-section, steps of the PFAHP are provided. In the second sub-section, the PFTOPSIS method that is used to assess the hazards presented. Finally, an overall picture of the proposed approach PFAHP and FTOPSIS methods is demonstrated.

PAHP

Based on the definitions given in "Pythagorean Fuzzy sets and related notations", procedural steps of PFAHP are presented in the following.

Step 1 The compromised pairwise comparison matrix $A = (a_{ik})_{\text{mxm}}$ is structured based on linguistic evaluations of experts using the scale proposed by Ilbahar et al. [32].

Step 2 The difference matrices $D = (d_{ik})_{\text{mxm}}$ between the lower and upper values of the membership and non-membership functions are calculated using Eqs. (8) and (9):

$$d_{ik_L} = \mu_{ik_L}^2 - v_{ik_U}^2, \tag{8}$$

$$d_{ik_U} = \mu_{ik_U}^2 - v_{ik_L}^2. \tag{9}$$

Step 3 Interval multiplicative matrix $S = (s_{ik})_{\text{mxm}}$ is computed using Eqs. (10) and (11):

$$s_{ik_L} = \sqrt{1000^{d_{ik_L}}}, \tag{10}$$

$$s_{ik_U} = \sqrt{1000^{d_{ik_L}}}. \tag{11}$$

Step 4 The determinacy value $\tau = (\tau_{ik})_{\text{mxm}}$ is calculated using Eq. (12):

$$\tau_{ik} = 1 - \left(\mu_{ik_U}^2 - \mu_{ik_L}^2\right) - \left(v_{ik_U}^2 - v_{ik_L}^2\right). \tag{12}$$

Step 5 The determinacy degrees are multiplied with $S = (s_{ik})_{\text{mxm}}$ matrix for obtaining the matrix of weights $T = (t_{ik})_{\text{mxm}}$ before normalization using Eq. (13):

$$t_{ik} = \left(\frac{s_{ik_L} + s_{ik_U}}{2}\right)\tau_{ik}. \tag{13}$$

Step 6 Each normalized priority weight w_i is computed using Eq. (14):

$$w_i = \frac{\sum_{k=1}^m t_{ik}}{\sum_{i=1}^m \sum_{k=1}^m t_{ik}}. \tag{14}$$

PFTOPSIS

PFTOPSIS is a multi-criteria decision-making (MCDM) technique based on the concept of choosing the solution with the shortest distance from the ideal solution and the farthest distance from the negative ideal solution by considering concept of Pythagorean fuzzy sets. The difference between FTOPSIS and intuitionistic fuzzy TOPSIS (IFTOPSIS) and PFTOPSIS is provided in Table 2.

Based on the definition and explanations above, the procedural steps of PFTOPSIS algorithm are provided in the following:

Step 1 In the first step, Pythagorean fuzzy number-based decision matrix $R = (C_j(x_i))_{mxn}$ is constructed. Here, $C_j(j = 1, 2, \ldots, n)$ and $x_i(i = 1, 2, \ldots, m)$ refer to values of criteria and alternatives. The matrix form is as follows:

$$R = (C_j(x_i))_{mxn} = \begin{pmatrix} P(u_{11}, v_{11}) & P(u_{12}, v_{12}) & \ldots & P(u_{1n}, v_{1n}) \\ P(u_{21}, v_{21}) & P(u_{22}, v_{22}) & \ldots & P(u_{2n}, v_{2n}) \\ \vdots & \vdots & \vdots & \vdots \\ P(u_{m1}, v_{m1}) & P(u_{m2}, v_{m2}) & \ldots & P(u_{mn}, v_{mn}) \end{pmatrix}.$$

Step 2 In the second step, Pythagorean fuzzy positive ideal solution (PIS) and negative ideal solutions (NIS) are determined using Eqs. (15, 16) as follows:

$$x^{+}=\left\{C_j,\max_i\langle s(C_j(x_i))\rangle | j=1,2,\ldots,n\right\}$$
$$=\left\{\langle C_1,P(u_1^{+},v_1^{+})\rangle,\langle C_2,P(u_2^{+},v_2^{+})\rangle,\ldots,\langle C_n,P(u_n^{+},v_n^{+})\rangle\right\},\tag{15}$$

$$x^{-}=\left\{C_j,\min_i\langle s(C_j(x_i))\rangle | j=1,2,\ldots,n\right\}$$
$$=\left\{\langle C_1,P(u_1^{-},v_1^{-})\rangle,\langle C_2,P(u_2^{-},v_2^{-})\rangle,\ldots,\langle C_n,P(u_n^{-},v_n^{-})\rangle\right\}.\tag{16}$$

Step 3 In the third step, distances from Pythagorean fuzzy PIS and NIS are determined using Eqs. (17, 18) as follows:

$$D(x_i,x^{+})=\sum_{j=1}^{n}w_j d(C_j(x_i),C_j(x^{+}))$$
$$=\frac{1}{2}\sum_{j=1}^{n}w_j\left(\left|(\mu_{ij})^2-(\mu_j^{+})^2\right|+\left|(v_{ij})^2-(v_j^{+})^2\right|\right.$$
$$\left.+\left|(\pi_{ij})^2-(\pi_j^{+})^2\right|\right),\tag{17}$$

$$D(x_i,x^{-})=\sum_{j=1}^{n}w_j d(C_j(x_i),C_j(x^{-}))$$
$$=\frac{1}{2}\sum_{j=1}^{n}w_j\left(\left|(\mu_{ij})^2-(\mu_j^{-})^2\right|+\left|(v_{ij})^2-(v_j^{-})^2\right|\right.$$
$$\left.+\left|(\pi_{ij})^2-(\pi_j^{-})^2\right|\right).\tag{18}$$

for Eqs. (17, 18) $i=1,2,\ldots,n$. In general, the smaller $D(x_i,x^{+})$ the better the alternative x_i and the bigger $D(x_i,x^{-})$ the better the alternative x_i and let $D_{\text{min}}(x_i,x^{+})=\min_{1\le i\le m}D(x_i,x^{+})$ and $D_{\text{max}}(x_i,x^{-})=\max_{1\le i\le m}D(x_i,x^{-})$.

Step 4 In the fourth step, the revised closeness $\xi(x_i)$ of the alternative x_i is computed using Eq. (19) as follows:

$$\xi(x_i)=\frac{D(x_i,x^{-})}{D_{\text{max}}(x_i,x^{-})}-\frac{D(x_i,x^{+})}{D_{\text{min}}(x_i,x^{+})}.\tag{19}$$

Step 5 In the fifth step, the best ranking order of the alternatives is determined. The alternative with the highest revised coefficient value is the best alternative.

Overall picture of the proposed approach

An RA process is especially followed by the steps of hazard identification, risk assessment, reducing risks, risk-residuals analysis, and selection of risk control options. Hazard identification step includes determining risks caused by potential hazards. The RA step is to calculate risk value based on three parameters of risk likelihood, risk severity and value of information. The value of information parameter is a special parameter for information security RA that refers to the sum of three factors as privacy, integrity, and accessibility. The risk reduction step enables the process to become more efficient so that significant risks are fast eliminated using hazard control hierarchy. After the risk reduction a second assessment is carried out to validate that the selected measures reduce the risks effectively. This is the step of assessing residual risks. The overall process follows a decision step hereafter. The risk assessment team decides on that the risks are reduced to an acceptable level by some control options. The structure of the proposed integrated approach followed in this study is given in Fig. 1.

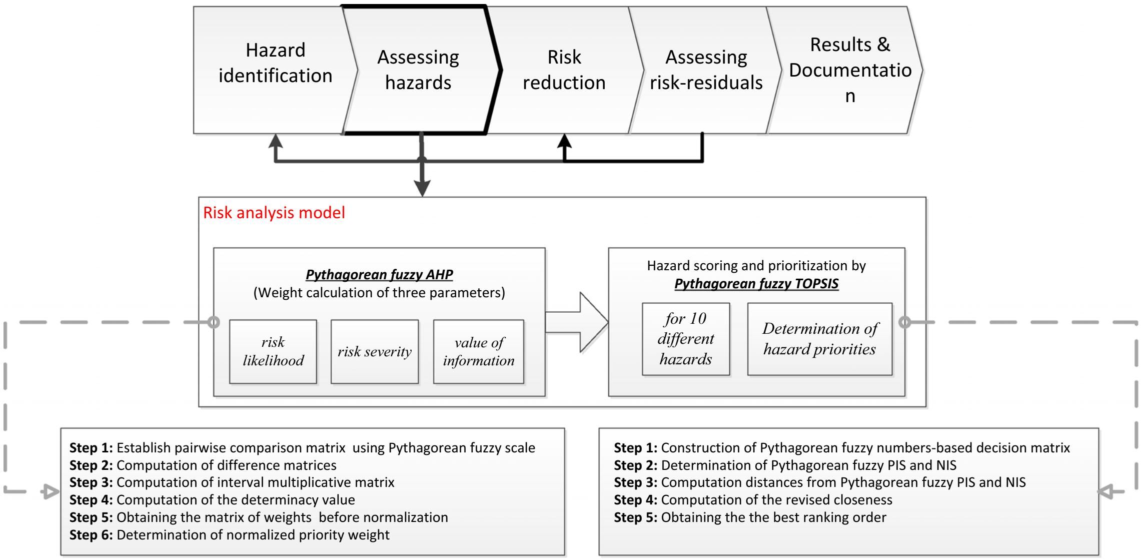
Case study: information security RA for corrugated cardboard sector

The observed facility and risks

The observed production facility is one of the biggest companies in the corrugated cardboard industry of Turkey with its domestic capital. The main activity of the factory is the production of corrugated cardboard and corrugated cardboard boxes (printed and unprinted). One of the basic management policies of the firm is to provide a safe working environment through proactive activities related to occupational health and safety. In this context, firstly, a RA team consisting of six experts with different sector experience levels is established. Then, potential information security hazards and their corresponding risks are identified in terms of maintenance and repair process of the corrugated cardboard production facility. A total of ten risks are identified by the expert team. The list of potential hazards associated within the maintenance and repair operations is provided in Table 3.

Application of the proposed approach

The second step of an RA process is regarding assessing the hazards and associated risks. In this step, PFAHP is used in weighing three risk parameters by taking into consideration pairwise comparison and fuzzy linguistic ratings. In the literature, classic RA methods mostly consider equal weights to two (e.g., likelihood and severity in decision matrix method), three (e.g., likelihood, severity and frequency in Fine–Kinney method and likelihood, severity and detection in FMEA method) or more risk parameters. Besides, different combinations of judgments on the parameters may lead to a completely different meaning. For example, hazards with high likelihood and low severity could be classified at the same level as hazards with low likelihood and high severity.



Step 1: Establish pairwise comparison matrix using Pythagorean fuzzy scale
Step 2: Computation of difference matrices
Step 3: Computation of interval multiplicative matrix
Step 4: Computation of the determinacy value
Step 5: Obtaining the matrix of weights before normalization
Step 6: Determination of normalized priority weight

Step 1: Construction of Pythagorean fuzzy numbers-based decision matrix
Step 2: Determination of Pythagorean fuzzy PIS and NIS
Step 3: Computation distances from Pythagorean fuzzy PIS and NIS
Step 4: Computation of the revised closeness
Step 5: Obtaining the the best ranking order

Fig. 1 The flow of proposed integrated RA approach

Table 3 Descriptions of the risks in information security RA of maintenance and repair process

Risk ID	Description of the hazard	Description of associated risk
ISR1	Loss of repairing papers	Historical data loss, delay in the plans of past jobs
ISR2	Loss of breakdown forms	Non-execution of analysis on changing parts and failures
ISR3	Non-execution of maintenance	Production stops, additional cost
ISR4	Intervention to electrical faults late	Increase in downtime
ISR5	Loss of scheduled maintenance papers	Failure in manufacturing, error, stops as a result of non-execution of daily, weekly, monthly and annual maintenance plans of the machines
ISR6	Loss of authorized staff, working with inexperienced staff	Increase in downtime
ISR7	Non-availability of spare parts	Increase in downtime, production stops
ISR8	Extension of spare parts procurement period	Customer loss, production stops due to non-availability of no spare parts in a possible failure
ISR9	Not to record all improvements, dependence on person, not to follow	Not having an organizational memory
ISR10	The absence of an area where copies of investment projects and copies of all the documents in all facilities are not available, not followed, no backup of soft documents on the common server	Declassifying of investment plans

These minuses are articulated in the literature [41]. So, this study considers weighting of the three parameters by interval-valued Pythagorean fuzzy numbers-based AHP. The priority orders of ten different hazards with respect to these parameters are then determined using PFTOPSIS (see Fig. 1). Data of the information security risks are taken from the expert team working in the corrugated cardboard production facility. This team first evaluates and rates the risk parameters in a pair wise systematic. Then, they rate risks with respect to the previously evaluated risk parameters. Due to space limitations, the evaluation forms are not included here. Readers can find all forms in Supplementary file.

The procedure explained in “Proposed integrated approach” shows the computational processes to derive the importance weights of three risk parameters. Six experts are asked to express their pairwise comparisons for each

Table 4 Weighing scale for PFAHP [32]

Linguistic term	Interval-valued Pythagorean fuzzy numbers			
	μ_L	μ_U	ν_L	ν_U
Certainly low important (CLI)	0.00	0.00	0.90	1.00
Very low important (VLI)	0.10	0.20	0.80	0.90
Low important (LI)	0.20	0.35	0.65	0.80
Below average important (BAI)	0.35	0.45	0.55	0.65
Average important (AI)	0.45	0.55	0.45	0.55
Above average important (AAI)	0.55	0.65	0.35	0.45
High important (HI)	0.65	0.80	0.20	0.35
Very high important (VHI)	0.80	0.90	0.10	0.20
Certainly high important (CHI)	0.90	1.00	0.00	0.00
Exactly equal (EE)	0.1965	0.1965	0.1965	0.1965

Table 8 The determinacy value matrix (τ)

Risk parameter	Likelihood	Severity	Value of information
Likelihood	1.000	0.894	0.960
Severity	0.894	1.000	0.800
Value of information	0.960	0.800	1.000

Table 9 Matrix of weights before normalization (t)

Risk parameter	Likelihood	Severity	Value of information
Likelihood	1.000	0.829	0.963
Severity	0.996	1.000	1.198
Value of information	0.963	0.601	1.000

risk parameter using the linguistic variables defined in Table 4.

In this stage, the linguistic variables are transferred into corresponding interval-valued Pythagorean fuzzy numbers. Since the ratings of these evaluators are different, it is required to aggregate their subjective judgments towards a compromised pairwise comparison matrix A as indicated in Step 1 of "Proposed integrated approach". The aggregated compromised pairwise comparison matrix for three parameters is given in Table 5. The difference matrix D and interval multiplicative matrix S are also given in Tables 6 and 7, respectively. The determinacy value matrix as stated in Eq. (12) and matrix of weights before normalization as in Eq. (13) are given in Tables 8 and 9, respectively.

Table 5 Aggregated compromised pairwise comparison evaluation of experts in matrix form

Risk parameter	Interval-valued Pythagorean fuzzy numbers: ⟨[degree of membership],[degree of non-membership]⟩ $\langle[\mu_L, \mu_u], [\nu_L, \nu_U]\rangle$		
	Likelihood	Severity	Value of information
Likelihood	⟨[0.197, 0.197], [0.197, 0.197]⟩	⟨[0.349, 0.416], [0.382, 0.449]⟩	⟨[0.281, 0.314], [0.281, 0.314]⟩
Severity	⟨[0.382, 0.449], [0.349, 0.416]⟩	⟨[0.197, 0.197], [0.197, 0.197]⟩	⟨[0.500, 0.600], [0.400, 0.500]⟩
Value of information	⟨[0.281, 0.314], [0.281, 0.314]⟩	⟨[0.400, 0.500], [0.500, 0.600]⟩	⟨[0.197, 0.197], [0.197, 0.197]⟩

Table 6 The difference matrix

Risk parameter	Likelihood	Severity	Value of information
Likelihood	⟨[0.000, 0.000]⟩	⟨[−0.080, 0.027]⟩	⟨[−0.020, 0.020]⟩
Severity	⟨[−0.027, 0.080]⟩	⟨[0.000, 0.000]⟩	⟨[0.000, 0.200]⟩
Value of information	⟨[−0.020, 0.020]⟩	⟨[−0.020, 0.000]⟩	⟨[0.000, 0.000]⟩

Table 7 The interval multiplicative matrix

Risk parameter	Likelihood	Severity	Value of information
Likelihood	⟨[1.000, 1.000]⟩	⟨[0.759, 1.096]⟩	⟨[0.934, 1.071]⟩
Severity	⟨[0.912, 1.317]⟩	⟨[1.000, 1.000]⟩	⟨[1.000, 1.995]⟩
Value of information	⟨[0.934, 1.071]⟩	⟨[0.501, 1.000]⟩	⟨[1.000, 1.000]⟩

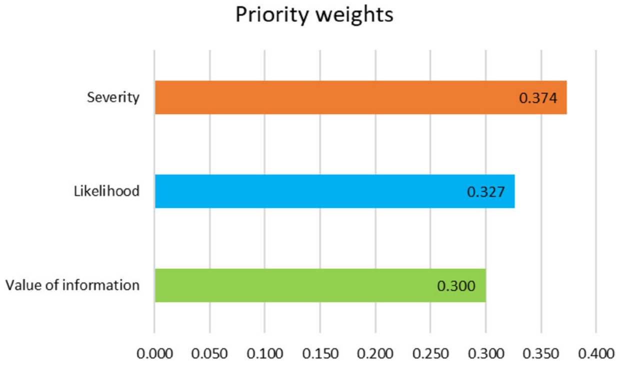


Fig. 2 Priority weights of three risk parameters by PFAHP

Table 10 Nine-point Pythagorean fuzzy linguistic scale for assessing risks [49]

Linguistic term	Corresponding Pythagorean fuzzy number (u, v)
Extremely low (EL)	(0.10, 0.99)
Very little (VL)	(0.10, 0.97)
Little (L)	(0.25, 0.92)
Middle little (ML)	(0.40, 0.87)
Middle (M)	(0.50, 0.80)
Middle high (MH)	(0.60, 0.71)
Big (B)	(0.70, 0.60)
Very tall (VT)	(0.80, 0.44)
Tremendously high (TH)	(0.10, 0.00)

Finally, the normalized priority weights of risk parameters are computed using Eq. (14) as shown in Fig. 2.

In the second stage, using these risk parameters' weights, and the evaluations of hazards with respect to each risk parameter, the PFTOPSIS is applied. The expert group evaluated ten hazards using linguistic variables and corresponding Pythagorean fuzzy numbers as shown in Table 10. At the end of this evaluation, the Pythagorean fuzzy decision matrix is constructed as in Table 11.

Then, using Eqs. (15, 16), Pythagorean fuzzy PIS and Pythagorean fuzzy NIS values are determined. The obtained results are as follows:

$$x^{+} = \left\{P(0.325, 0.895),\ P(0.517, 0.782),\ P(0.567, 0.737)\right\}$$

$$x^{-} = \left\{P(0.100, 0.987),\ P(0.125, 0.965),\ P(0.100, 0.977)\right\}.$$

Then, employing Eqs. (17, 18), distances from Pythagorean fuzzy PIS and NIS are calculated. The results are provided in Table 12. Moreover, the revised closeness values are computed using Eq. (19) and the results are also listed in Table 12. According to these revised closeness values, ranking of hazards is obtained as shown in Fig. 3.

Table 11 Pythagorean fuzzy decision matrix

Risk ID	Likelihood	Severity	Value of information
ISR1	P (0.1, 0.977)	P (0.15, 0.957)	P (0.1, 0.977)
ISR2	P (0.125, 0.965)	P (0.125, 0.962)	P (0.125, 0.965)
ISR3	P (0.125, 0.965)	P (0.517, 0.782)	P (0.2, 0.937)
ISR4	P (0.125, 0.968)	P (0.383, 0.863)	P (0.225, 0.928)
ISR5	P (0.1, 0.977)	P (0.225, 0.928)	P (0.1, 0.973)
ISR6	P (0.225, 0.928)	P (0.3, 0.903)	P (0.225, 0.928)
ISR7	P (0.225, 0.935)	P (0.358, 0.872)	P (0.3, 0.903)
ISR8	P (0.325, 0.895)	P (0.458, 0.817)	P (0.433, 0.847)
ISR9	P (0.1, 0.987)	P (0.125, 0.965)	P (0.458, 0.817)
ISR10	P (0.125, 0.965)	P (0.15, 0.953)	P (0.567, 0.737)

P (u, v) refers to a Pythagorean fuzzy number

Table 12 Results obtained by the PFTOPSIS

Risk ID	$D\,(X_i, X^{+})$		$D\,(X_i, X^{-})$		ξ (X$_i$)
ISR1	$D\,(X_1, X^{+})$	0.287	$D\,(X_1, X^{-})$	0.083	– 3.605
ISR2	$D\,(X_2, X^{+})$	0.276	$D\,(X_2, X^{-})$	0.088	– 3.443
ISR3	$D\,(X_3, X^{+})$	0.143	$D\,(X_3, X^{-})$	0.222	– 1.148
ISR4	$D\,(X_4, X^{+})$	0.190	$D\,(X_4, X^{-})$	0.176	– 1.960
ISR5	$D\,(X_5, X^{+})$	0.265	$D\,(X_5, X^{-})$	0.105	– 3.228
ISR6	$D\,(X_6, X^{+})$	0.192	$D\,(X_6, X^{-})$	0.161	– 2.036
ISR7	$D\,(X_7, X^{+})$	0.161	$D\,(X_7, X^{-})$	0.196	– 1.494
ISR8	$D\,(X_8, X^{+})$	0.073	$D\,(X_8, X^{-})$	0.278	0.000
ISR9	$D\,(X_9, X^{+})$	0.213	$D\,(X_9, X^{-})$	0.163	– 2.316
ISR10	$D\,(X_{10}, X^{+})$	0.154	$D\,(X_{10}, X^{-})$	0.211	– 1.336

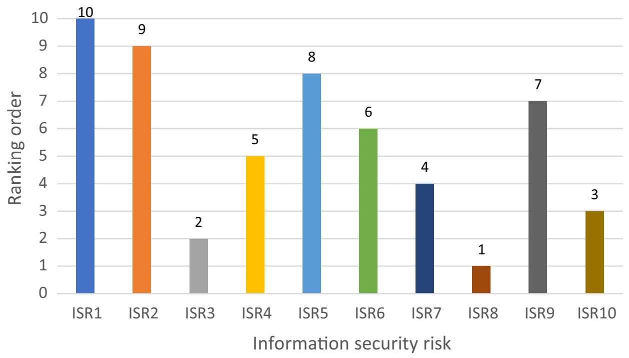


Fig. 3 Ranking orders of information security risks in the maintenance and repair process of a corrugated cardboard production facility

Table 13 Likelihood ratings

Value	Description of the likelihood parameter
1	Very low; there is no threat to be tested
2	Low; the threat can rarely occurr
3	Medium; the threat can occurr
4	High; the threat is often repeated.
5	Very high; the threat is not to be avoided

Table 14 Severity ratings

Value	Description of the severity parameter
1	Very low; damage that does not directly affect the operation
2	Low; damage that affects activity but does not interrupt
3	Medium; damage that interrupts activity in an insignificant level
4	High; damage that disrupts the activity to a loss of reputation
5	Very high; damage that endangers institutional sustainability

It is shown in Fig. 3 that the most important five identified hazards for information security RA of maintenance and repair process are ISR8 (extension of spare parts procurement period), ISR3 (non-execution of maintenance), ISR10 (the absence of an area where copies of investment projects and copies of all the documents in all facilities are not available, not followed, no backup of soft documents on the common server), ISR7 (non-availability of spare parts) and ISR4 (intervention to electrical faults late).

Comparison of the results

To validate the efficiency of the proposed integrated approach, a comparison study is performed with classical method that the facility followed, PFAHP–PFVIKOR integration and PAHP–PFMOORA integration. According to the followed classical RA, three parameters are combined for risk score. The parameters are severity (S), likelihood (L) and value of information (Vof$I$). The risk score is calculated by multiplexing these three parameters. Parameter of VofI is a special parameter for the information security RA. It combines three factors of privacy (P), integrity (I), and accessibility (A). The calculation of this parameter is to sum of three factors. For each of the parameters, a five-point scale is available as given in Tables 13, 14 and 15.

The evaluation of information security risks done by the facility executives and the ranking results using the ratings in Tables 13, 14 and 15 are represented in Table 16. Risk scores of 10 information risks were obtained. Risk score with a value of 108 (ISR8) is the most important risk. ISR10 with a score value of 96 is placed at the second rank. ISR7 and ISR4 are followed by this risk with score values of 84 and 72 and clustered in the third and fourth ranking orders. ISR6 with a score value of 54 is the fifth most important risk. Two risks fell in the sixth ranking order that have a risk value of 48. ISR1, ISR2, and ISR5 are the least important hazards with a score value of 12.

To provide a more visual comparison between the proposed integrated approach and the other three approaches, the ranking order results of each approach can be demonstrated visually in Fig. 4.

The first comparison analysis is conducted between the proposed approach and classical method. The comparison shows that, the ranking orders of information security risks are partially different from the proposed integrated approach. The ranking orders of risks ISR3, ISR4, ISR6, ISR7, and ISR10 are different between the two approaches. According to the Fig. 4, ISR ranks the first in terms of both approaches. The ranking order of the least important risks is partially the same.

The second comparison analysis is performed between the ranking order results obtained by the integration based on PFAHP and PFVIKOR and the proposed RA approach. It can be seen that information security risks ISR8, ISR3, ISR10, and ISR7 have the highest priority ranking orders in the proposed approach. It is consistent with the ranking results of PFAHP–PFVIKOR integrated approach. In addition, the hazards ISR1, ISR2, and ISR have the lowest risk priority ranking orders in the proposed approach. It is also consistent with the PFAHP–PFVIKOR integrated approach.

The third comparison is carried with the integration based on PFAHP and PFMOORA. From Fig. 4, the risk priority ranking results by the proposed approach and PFAHP–PFMOORA-integrated approach are similar to the second comparison. That is, the first three information security risks and the last two risks remain the same in both approaches.

In addition, a correlation coefficient is applied to measure the correlation between the final risk score values of classical method, ξ values of the proposed integrated approach, final VIKOR score values (Q values) and final MOORA score values. The outputs of correlation analysis are demonstrated in Table 17.

According to results in Table 17, the relationships between ranking results are very strong. In PFAHP–PFVIKOR approach, a higher index value shows a lower ranking order. Hence, the correlation coefficient between PFAHP–PFVIKOR approach and the remaining approaches is a negative, high value as tabulated in Table 17. The correlation coefficient between the proposed approach and PFAHP–PFMOORA approach is positive and the highest of all approaches (0.99). The lowest correlation coefficient val-

Table 15 Ratings of privacy, integrity, and accessibility

Value	Privacy descriptions	Integrity descriptions	Accessibility descriptions
1	Critical information will not be released if there is damage to the asset. The level of criticality of the information that emerges does not affect the institution	In the event of a damage to the asset, the critical information changes out of control. The level of criticality of the information that changes outside of control is not affected	Critical information can be accessed if there is damage to the asset. The level of criticality of information that hurts accessibility does not affect the organization
2	Critical information will not be released if there is damage to the asset. The level of criticality of the information that emerges affects the institution. Impact can be compensated in the short term	In the event of a damage to the asset, the critical information does not change out of control. The level of criticality of information that changes outside control is affecting the organization. Impact can be compensated in the short term	Critical information can be accessed if there is damage to the asset. The level of criticality of information that hurts accessibility impacts the organization. Impact can be compensated in the short term
3	Critical information will not be released if there is damage to the asset. The level of criticality of the information that emerges affects the institution. The effect can be compensated in the medium term	In the event of a damage to the asset, the critical information changes out of control. The level of criticality of information that changes outside control is affecting the organization. Impact can be compensated in the short term	Critical information can be accessed if there is damage to the asset. The level of criticality of information that hurts accessibility impacts the organization. Impact can be compensated in the short term
4	Critical information comes to light if there is damage to the asset. The level of criticality of the information that emerges affects the institution. The effect can be compensated in the medium term	In the event of a damage to the asset, the critical information changes out of control. The level of criticality of information that changes outside control is affecting the organization. The effect can be compensated in the medium term	Critical information is inaccessible if there is damage to the asset. The level of criticality of information that hurts accessibility impacts the organization. The effect can be compensated in the medium term
5	Critical information comes to light if there is damage to the asset. The level of criticality of the information that emerges affects the institution. The effect cannot be compensated or compensated in the long run	In the event of a damage to the asset, the critical information changes out of control. The level of criticality of information that changes outside control is affecting the organization. The effect cannot be compensated, but it can be compensated in the long run	Critical information is inaccessible if there is damage to the asset. The level of criticality of information that hurts accessibility impacts the organization. The effect cannot be compensated or compensated in the long run

Table 16 Evaluations of the information security risks by means of the classical method followed by facility

Risk ID	Value of information (Vof$I$)			(Vof$I$) = $(P)+(I)+(A)$	Severity (S)	Likelihood (L)	Risk score value (S)*(L)*$[(P)+(I)+(A)]$
	Privacy (P)	Integrity (I)	Accessibility (A)				
ISR1	2	2	2	6	2	1	12
ISR2	2	2	2	6	2	1	12
ISR3	2	2	2	6	4	2	48
ISR4	3	3	3	9	4	2	72
ISR5	2	2	2	6	2	1	12
ISR6	2	2	2	6	3	3	54
ISR7	3	2	2	7	4	3	84
ISR8	3	3	3	9	3	4	108
ISR9	4	4	4	12	2	2	48
ISR10	4	4	4	12	4	2	96

ues are obtained from the comparisons of classical method with others (0.91 and -0.92). This indicates the weakness of classical method. In contrast, the proposed approach can overcome this disadvantage associated with the classical method. According to the results, it is proved that the proposed approach can produce reasonable results and provide suitable information to assist management in the risk assessment problems.

The above-obtained results indicate the effectiveness and easiness of the model to prefer proposed model rather than

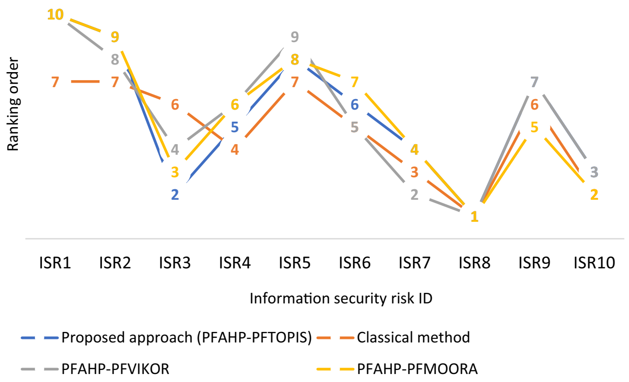


Fig. 4 Ranking order results of information security risk in terms of four approaches

classical model for the company. Firstly, it is very important that the information security risk analysis on the managerial basis requires the highest level of security and detailed work. The proposed method offers a much more detailed analysis than the classical model. Secondly information security risk analysis also has great importance as it will create a table to show which security measures will be taken on an administrative basis. On the other hand, information security is also important as an element of corporate governance. It should be recognized that the priority must be high, as it has obligations to employees, business partners, and customers. Therefore, it is important for each employee to pay attention to confidentiality, integrity, and usability of corporate and personal information assets in terms of criticality, sensitivity, importance, and value levels. It can be observed that proposed model has significant advantages over classical risk assessment models.

Conclusion

Classical RA methods are commonly applied in various workplaces for health, safety, and security problems. These methods determine the score of risk parameters (mostly parameters of severity and probability) using crisp values, assume the risk parameters as independent and produce the same risk value by different combinations of risk parameters' scores. All these mentioned shortcomings require proposal of a new and novel RA methodology that can improve effectiveness in practical risk management. In this paper, a new RA methodology is proposed based on AHP–TOPSIS integration extended with Pythagorean fuzzy sets and applied to the information security RA. The interval-valued PFAHP is used to calculate the weights of risk parameters. A new parameter specific to information security RA is considered in this study for the first time. The parameters are risk likelihood, risk severity, and value of information. The value of information parameter refers to the sum of three factors as privacy, integrity, and accessibility. The risk priority of each hazard is calculated using the PFTOPSIS. A case study on the assessment of risks was carried out for maintenance and repair process in corrugated cardboard sector. According to the comparison study, it can be summarized that the proposed method can provide more reasonable and precise calculation of risk values in classical method, as well as improve the effectiveness of the classical RA method that the observed facility follows.

In summary, contributions of the current study to the literature are as follows:

- A new risk parameter for information security RA called value of knowledge is considered for the first time in the literature.
- The PFAHP and PFTOPSIS, which are commonly used MADM methods with Pythagorean fuzzy sets, are applied integrally to the assessment of risks for the first time in the literature. By doing this, an upgraded fuzzy MADM-based RA approach using linguistic terms with Pythagorean fuzzy set theory has been implemented. Use of Pythagorean fuzzy sets successfully managed the uncertainty and vagueness of the expert teams' perceptions during the subjective judgment process.
- A comparative analysis with classical RA method, PFAHP–PFVIKOR, PFAHP–PFMOORA approach that the observed facility followed is carried out. Results of this analysis proved that the proposed approach can produce reasonable results and provide suitable information to assist management in the risk assessment problems.

Table 17 Correlation coefficient results of the compared approaches

	Classical method	Proposed approach (PFAHP–PFTOPIS)	PFAHP–PFVIKOR	PFAHP–PFMOORA
Classical method	1			
Proposed approach (PFAHP–PFTOPIS)	0.91	1		
PFAHP–PFVIKOR	– 0.92	– 0.97	1	
PFAHP–PFMOORA	0.91	0.99	– 0.964	1

Although the study has contributions, it has some limitations. Subjective evaluation of both risk parameters and hazards depends on safety expert's experience. This may make the RA results different. Therefore, an objective evaluation procedure can be followed such as, making a different weighing among experts, using different risk parameter weights for evaluation of each hazard and proposing an optimized way in determination of each risk parameter. Another future direction may be using the proposed RA approach to address risk evaluation problems in other practical cases.

References

1. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality based beliefs and information security awareness. MIS Q 34(3):523–548
2. Anderson RJ (2001) Why information security is hard—an economic perspective. In: 17th annual computer security applications conference, pp 358–365
3. Bones E, Hasvold P, Henriksen E, Strandenes T (2007) "Risk analysis of information security in a mobile instant messaging and presence system for healthcare. Int J Med Inform 76:677–687
4. Karabacak B, Sogukpinar I (2005) ISRAM: information security risk analysis method. Comput Secur 24(2):147–159
5. Eloff JH, Labuschagne L, Badenhorst KP (1993) A comparative framework for risk analysis methods. Comput Secur 12(6):597–603
6. Spears J (2006) A holistic risk analysis method for identifying information security risks. Security management integrity and internal control in information systems, vol 193. Boston Springer, Boston, pp 185–202
7. Webb J, Ahmad A, Maynard SB, Shanks G, Popovski P (2014) A situation awareness model for information security risk management. Comput Secur 44:1–15
8. Garg H (2018) A linear programming method based on an improved score function for interval-valued pythagorean fuzzy numbers and its application to decision-making. Int J Uncertain Fuzziness Knowl Based Syst 26(01):67–80
9. Garg H (2018) Linguistic Pythagorean fuzzy sets and its applications in multiattribute decision-making process. Int J Intell Syst 33(6):1234–1263
10. Garg H (2018) New Logarithmic operational laws and their aggregation operators for Pythagorean fuzzy set and their applications. Int J Intell Syst. https://doi.org/10.1002/int.22043
11. Garg H (2018) New exponential operational laws and their aggregation operators for interval valued Pythagorean fuzzy multicriteria decision-making. Int J Intell Syst 33(3):653–683
12. Garg H (2018) Some methods for strategic decision-making problems with immediate probabilities in Pythagorean fuzzy environment. Int J Intell Syst 33(4):687–712
13. Gul M, Ak MF, Guneri AF (2017) Occupational health and safety risk assessment in hospitals: a case study using two-stage fuzzy multi-criteria approach. Hum Ecol Risk Assess Int J 23(2):187–202
14. Gul M, Celik E, Akyuz E (2017) A hybrid risk-based approach for maritime applications: the case of ballast tank maintenance. Hum Ecol Risk Assess Int J 23(6):1389–1403
15. Gul M (2018) A review of occupational health and safety risk assessment approaches based on multi-criteria decision-making methods and their fuzzy versions. Hum Ecol Risk Assess Int J 24(7):1723–1760
16. Gul M, Guneri AF (2016) A fuzzy multi criteria risk assessment based on decision matrix technique: a case study for aluminum industry. J Loss Prev Process Ind 40:89–100
17. Gul M, Guneri AF (2018) Use of FAHP for occupational safety risk assessment: an application in the aluminum extrusion industry. In: Emrouznejad A, Ho W (eds) Fuzzy analytic hierarchy process. CRC Press, Taylor & Francis Group, pp 249–271
18. Gul M, Guneri AF, Baskan M (2018) An occupational risk assessment approach for construction and operation period of wind turbines. Glob J Environ Sci Manag 4(3):281–298
19. Gul M, Guven B, Guneri AF (2018) A new Fine–Kinney-based risk assessment framework using FAHP-FVIKOR incorporation. J Loss Prev Process Ind 53:3–16
20. Guneri AF, Gul M, Ozgurler S (2015) A fuzzy AHP methodology for selection of risk assessment methods in occupational safety. Int J Risk Assess Manag 18(3–4):319–335
21. Oz NE, Mete S, Serin F, Gul M (2018) Risk assessment for clearing & grading process of a natural gas pipeline project: an extended TOPSIS model with Pythagorean fuzzy sets for prioritizing hazards. Hum Ecol Risk Assess Int J. https://doi.org/10.1080/10807039.2018.1495057
22. Ozdemir Y, Gul M, Celik E (2017) Assessment of occupational hazards and associated risks in fuzzy environment: a case study of a university chemical laboratory. Hum Ecol Risk Assess Int J 23(4):895–924
23. Feng DG, Zhang Y, Zhang YQ (2004) Survey of information security risk assessment. J China Inst Commun 25(7):10–18
24. Ngai EWT, Wat FKT (2005) Fuzzy decision support system for risk analysis in E-commerce development. Decis Support Syst 40(2):235–255
25. Gul M, Celik E (2018) Fuzzy rule-based Fine–Kinney risk assessment approach for rail transportation systems. Hum Ecol Risk Assess Int J 24(7):1786–1812
26. De Gusmao APH, Silva LCE, Silva MM, Poleto T, Costa APCS (2016) Information security risk analysis model using fuzzy decision theory. Int J Inf Manag 36(1):25–34
27. Öğütçü G, Testik ÖM, Chouseinoglou O (2016) Analysis of personal information security behavior and awareness. Comput Secur 56:83–93
28. Gul M, Ak MF (2018) A comparative outline for quantifying risk ratings in occupational health and safety risk assessment. J Clean Prod 196:653–664
29. Carpitella S, Certa A, Izquierdo J, La Fata CM (2018) A combined multi-criteria approach to support FMECA analyses: a real-world case. Reliab Eng Syst Saf 169:394–402
30. Yager RR (2014) Pythagorean membership grades in multicriteria decision making. IEEE Trans Fuzzy Syst 22(4):958–965
31. Gul M (2018) Application of Pythagorean fuzzy AHP and VIKOR methods in occupational health and safety risk assessment: the case of a gun and rifle barrel external surface oxidation and colouring unit. Int J Occup Saf Ergon. https://doi.org/10.1080/10803548.2018.1492251
32. Ilbahar E, Karaşan A, Cebi S, Kahraman C (2018) A novel approach to risk assessment for occupational health and safety using Pythagorean fuzzy AHP & fuzzy inference system. Saf Sci 103:124–136
33. Karasan A, Ilbahar E, Cebi S, Kahraman C (2018) A new risk assessment approach: safety and critical effect analysis (SCEA) and its extension with Pythagorean fuzzy sets. Saf Sci 108:173–187

34. Mohd WRW, Abdullah L (2017) Pythagorean fuzzy analytic hierarchy process to multi-criteria decision making. In: AIP conference proceedings, vol 1905, no 1, p 040020. AIP Publishing
35. Zeng S, Chen J, Li X (2016) A hybrid method for pythagorean fuzzy multiple-criteria decision making. Int J Inf Technol Decis Mak 15(02):403–422
36. Zhang X, Xu Z (2014) Extension of TOPSIS to multiple criteria decision making with Pythagorean fuzzy sets. Int J Intell Syst 29(12):1061–1078
37. Garg H (2016) A new generalized Pythagorean fuzzy information aggregation using Einstein operations and its application to decision making. Int J Intell Syst 31(9):886–920
38. Garg H (2016) A novel accuracy function under interval-valued Pythagorean fuzzy environment for solving multicriteria decision making problem. J Intell Fuzzy Syst 31(1):529–540
39. Garg H (2017) Confidence levels based Pythagorean fuzzy aggregation operators and its application to decision-making process. Comput Math Organ Theory 23(4):546–571
40. Garg H (2017) Generalized Pythagorean fuzzy geometric aggregation operators using Einstein t-norm and t-conorm for multicriteria decision-making process. Int J Intell Syst 32(6):597–630
41. Grassi A, Gamberini R, Mora C, Rimini B (2009) A fuzzy multi-attribute model for risk evaluation in workplaces. Saf Sci 47(5):707–716
42. Gul M, Guneri AF, Nasirli SM (2018) A fuzzy-based model for risk assessment of routes in oil transportation. Int J Environ Sci Technol. https://doi.org/10.1007/s13762-018-2078-z
43. Wang W, Liu X, Qin Y (2018) A fuzzy Fine–Kinney-based risk evaluation approach with extended MULTIMOORA method based on Choquet integral. Comput Ind Eng 125:111–123
44. Wang W, Liu X, Qin Y, Fu Y (2018) A risk evaluation and prioritization method for FMEA with prospect theory and Choquet integral. Saf Sci 110:152–163
45. Can GF, Toktas P (2018) A novel fuzzy risk matrix-based risk assessment approach. Kybernetes. https://doi.org/10.1108/K-12-2017-0497
46. Can GF (2018) An intuitionistic approach based on failure mode and effect analysis for prioritizing corrective and preventive strategies. Hum Factors Ergon Manuf Serv Ind. https://doi.org/10.1002/hfm.20729
47. Yazdi M (2017) Hybrid probabilistic risk assessment using fuzzy FTA and fuzzy AHP in a process industry. J Fail Anal Prev 17(4):756–764
48. Yazdi M, Kabir S (2017) A fuzzy Bayesian network approach for risk analysis in process industries. Process Saf Environ Prot 111:507–519
49. Pérez-Domínguez L, Rodríguez-Picón LA, Alvarado-Iniesta A, Luviano Cruz D, Xu Z (2018) MOORA under Pythagorean fuzzy set for multiple criteria decision making. Complexity. https://doi.org/10.1155/2018/2602376
50. Fattahi R, Khalilzadeh M (2018) Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment. Saf Sci 102:290–300