

## Research Article

# Compliance Risk Assessment in the Banking Sector: Application of a Novel Pairwise Comparison-Based PRISM Method

Ferenc Bognár <sup>1</sup>, Balázs Szentes <sup>2</sup>, and Petra Benedek <sup>1</sup>

<sup>1</sup>Department of Management and Business Economics, Faculty of Economic and Social Sciences, Budapest University of Technology and Economics, Műgyetem Rkp. 3, H-1111, Budapest, Hungary

<sup>2</sup>Department of Management, Faculty of Business and Economics, University of Pannonia, Egyetem Utca 10, H-8200, Veszprém, Hungary

Correspondence should be addressed to Ferenc Bognár; [bognar.ferenc@gtk.bme.hu](mailto:bognar.ferenc@gtk.bme.hu)

Received 1 July 2022; Revised 19 January 2023; Accepted 22 March 2023; Published 15 May 2023

Academic Editor: Siew Ann Cheong

Copyright © 2023 Ferenc Bognár et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Up-to-date compliance management uses a risk-based approach based on international standards. In addition to techniques and practices, implementing compliance measures is determined by principles and culture. Compliance risk assessment is an evolving field in theory and practice. Compliance risk management is complex and highly dependent on the decisions of experts. This article presents a new compliance risk assessment method based on a commercial banking case study. In the study, the Guilford method is used to extend the Partial Risk Map (PRISM) assessment technique, and the steps of the proposed pairwise comparison-based PRISM method are described in detail. Since risk assessment is critical to the operation and development of compliance management systems, the proposed risk assessment method involves testing individual evaluations' consistency and the results' robustness. The best-fitting and outlier experts can be identified based on testing the impact of individual expert rankings on the aggregated ranking. The main finding is that top partial risks can be identified by applying the proposed pairwise comparison-based PRISM technique; therefore, possible optimal risk mitigation strategies and measures can be designed.

## 1. Introduction

Compliance management is an organizational function responsible for fulfilling legal, regulatory, industrial, and other obligations. The compliance management function is usually independent and reports to top-level executives and the board [1]. Preferably, one person is formally responsible for operating the compliance management system (CMS). At the same time, the responsible department has a thorough knowledge and know-how of organizational operations, processes, and procedures. The maturity and scope of a CMS, the budget, and the workforce allocated demonstrate leadership's commitment to a compliant and trustworthy way of running the business.

The scope of compliance has recently expanded, and the approach of integrating operational and compliance risk,

one of the critical categories of banking risks, is becoming widespread [2, 3]. Compliance risk management involves understanding and quantifying risk tolerance and a system of indicators and alerts always unique for the organization. Compliance risks, including reputational risks, can increase strategic risks in the banking sector [4]. Studies showed that simplifying banking business models is necessary [5], and more consistent and cheaper compliance procedures could be made possible [3]. Compliance management is more than a bureaucratic fulfilment of requirements. It has a business dimension [6] with increasing importance and complexity. Its main challenges include a lack of dedicated local compliance experts, incomplete indicators, hidden risks in third-party relationships, and rapidly changing regulatory requirements (for example, COVID-19 pandemic social distancing, loan moratorium, and commercial sanctions) [7].

The compliance scope and activities are becoming highly complex in an increasingly fast-changing and globalized world. Thus, the risk assessment processes must be developed to keep up with the increasing complexity. The most cited risk assessment methods follow the requirements of the increasing complexity of the assessment process [8]. The two most popular ways include combining risk assessment approaches with Multi-Criteria Decision-Making (MCDM) methods and fuzzy applications to describe complex phenomena more accurately. As typical risk assessment techniques in many industries, risk matrices and the Failure Mode and Effect Analysis (FMEA) have numerous development directions in recent decades. As a novel risk assessment technique built on the factors of FMEA, the PRISM method focuses on assessing partial risks that can stay hidden and lead to severe effects [9]. Similar to the PRISM method, Ouyang et al. [10] also described a possible way to detect hidden risks. That method can also be a sound basis for bank compliance risk assessment.

As many references show [2, 4, 11, 12], the assessment of bank compliance risk is a significantly complex process that has many different evaluation factors. On the other hand, the existing methodological tools are just following the continuously gaining complexity of bank compliance assessment. Although some quantitative and deterministic approaches have already been described [2, 9] and PRISM method is focusing on hidden risk identification, many possible approaches still need to be added to the toolset, which could strengthen the methods' reliability in providing information related to the compliance risk set of a bank. In bank compliance management, hidden risks can seriously damage the organization's reputation, and spillover effects can cause a further threat to the entire sector [13].

The purpose of the study is to develop a novel PRISM risk assessment technique that can deal with the following criteria: the method should not use a deterministic scale-based risk assessment (1); the method can be applied for testing the consistency of the assessors (2); the similarities and dissimilarities of the assessors' results can be compared to each other in detail; thus, the uncertainty of the group level decision can be reduced (3); and the new method must provide the same ability in hidden risk detection than the initial PRISM method (4). With this improved skillset, the novel PRISM method can be a more robust approach to complex risk assessment just like bank compliance risk assessment.

The paper is organized as follows. Section 2 presents the compliance management and risk assessment background of the study. Section 3 introduces the proposed methodology in detail. Section 4 presents a case study in the banking sector and highlights the results of applying the method. Section 5 discusses the results. Finally, Section 6 summarizes the most important added values of the proposed methodology and propositions for future research.

## 2. Literature Review

First, the bank risk and compliance risk studies are presented. Next, the ISO 37301:2021 Compliance management

system standard is introduced. Then, the compliance risk assessment literature is summarized.

*2.1. Bank and Compliance Risk.* The Basel Committee on Banking Supervision introduced the risk-based approach in the banking sector; nowadays, it has become business as usual. According to [14], out of the four main bank risks (liquidity, interest rate, capital, and credit risk), credit risk is generally viewed as critical regarding its impact on bank performance and failure. However, according to [15], the relationship between the effectiveness of risk management and bank risk is more significant in countries with higher institutional quality and standards. Empirical studies show that countries with better institutional systems are less likely to experience a banking crisis [16] which goes hand in hand with economic crises.

Moral hazard is a significant problem in liberalized financial systems, where there are more risk-taking opportunities [17]. Regulatory and supervisory practices (e.g., accurate disclosure of information) contribute to the performance and stability of the bank [18]. Tran et al. [19] used accounting and market-based risk measures in their study, finding that bank risk is negatively related to credit information sharing, which reduces the adverse effects of credit shocks on bank stability.

A three-step procedure has been created by Bezrodna [4] for assessing the bank's strategic risk and supporting its relationship with the compliance risk of financial monitoring. One finding is that compliance risk triggers an increase in strategic risk due to the application of financial sanctions against the bank. These may lead to reputational risks, negatively affecting the strategy's effectiveness. Furthermore, a significant difference between the actual and planned values of the indicators, or the inadequacy of the bank's strategic management mechanism, may lead it to focus on a formal approach to compliance with financial monitoring legislation [4]. The work of Birindelli and Ferretti [20] describes the similarities between operational risk and compliance risk and identifies areas of collaboration to achieve cost synergies and improved operational efficiency.

Many research studies [21–24] suggest that the committees that meet regularly during the financial year are linked to effective monitoring. As a result, audit committee effectiveness can reduce risks and increase banks' stability for regulatory compliance [25]. However, another study by Nguyen [24] shows that the audit committee's independence, number of meetings, and financial expertise negatively affect the risk-taking behavior of traditional banks.

As for Islamic banks, Masood et al. [26] showed that they develop and practice more robust techniques to manage their credit risk in addition to traditional methods, compared to non-Islamic banks. Empirical evidence [27] shows that Islamic banks below the target risk level tend to exhibit risk-seeking behavior. Also, Islamic banks with a higher loan-to-total assets ratio tend to take lower risks. A model has been developed by Ashraf and Lahsasna [28] to quantify

the Shariah risk and the level of Shariah compliance taken by Islamic banks, which can supplement traditional counterparty risk rating models.

In addition, a higher frequency of Sharia committee meetings reduces the risk of Sharia noncompliance in Islamic banks [29]. The impact of political connections on Shariah compliance of Islamic banks was examined by Syaputri and Nainggolan [30], finding that politically connected banks can reduce the risk of Shariah noncompliance better than nonpolitically connected Islamic banks.

Compliance risk is any event with a negative legal or reputational consequence. Most businesses have a strategically defined appetite and tolerance for risk that depends on several factors. Moreover, risks have a spillover and multiplier effect and can reinforce each other. Salvioni et al. [11] proposed a responsibility-oriented approach to compliance risk management, claiming that the lack of ethics in business operations, masked by formal compliance, often results in indirect adverse effects on the relationships between stakeholders.

**2.2. Compliance Management Systems.** In 2021, the International Organization for Standardization (ISO) issued a new standard, the ISO 37301:2021 Compliance management systems—Requirements with guidance for use [31], that supersedes the ISO 19600:2014. The main change is shifting from guidelines to requirements and the possibility of certifying the CMS against the standards. The general elements of a CMS are shown in Figure 1.

The organization and its legal, social, and cultural context are fundamental to the compliance management system. Understanding the context means considering several issues, including the business model, size, and the complexity and sustainability of the organization's activities and operations [31].

Besides the effect of the context, the top part, namely, objectives and principles, has a significant effect on how a compliance management system is designed and developed. Out of the objectives, reputation should be highlighted. A good reputation is usually the result of years of excellent expertise and cannot be created overnight [32]. Therefore, management needs to be aware of the reputation and emphasize it as a business resource. Reputational capital is the part of market value attributed to a firm's view as a responsible corporation [33].

The principles of the CMS are integrity, good governance, proportionality, transparency, accountability, and sustainability. One goal of mature compliance management is ensuring the integrity of the entire organization and its employees through the organization's leadership and management system [34–36]. Integrating good governance with a risk-based compliance function can improve performance efficiency and effectiveness [37]. According to [38], creating an effective internal control environment can mitigate or eliminate risks to corporate sustainability. Though not expressed explicitly, Governance, Risk, and Compliance (GRC) is the dominant approach in the ISO 37301:2021.



FIGURE 1: A simplified presentation of the elements of a compliance management system (edited version of ISO 37301:2021).

The center of Figure 1 shows the PDCA cycle, a four-step improvement planning tool. Governance, in the middle, refers to the comprehensive system of rules, practices, and standards that govern an enterprise. Leadership and culture are connected to all steps of the development cycle.

Identifying potential threats to a business is part of the Plan phase. This phase includes determining the scope, creating compliance policies, and clarifying roles and responsibilities. Design of operations and identification of compliance risks are also included here. So what are compliance risks? According to ISO 37301, compliance risk is the likelihood of occurrence and the consequences of non-compliance with the organization's (mandatory or voluntary) compliance obligations [31]. A practical and developed CMS aims to minimize the risk and consequences of noncompliance with obligations. Creating commitment at all levels is another ongoing task in the massive step of planning.

Compliance in action creates and uses processes and controls to ensure that the company and its employees conduct their business legally and ethically. Taking action to reduce or eliminate the effects of compliance risks is part of the Do phase. This phase also includes raising awareness, providing communication channels, training to elevate competence, and documentation.

Internal compliance audits, management reviews, monitoring, and measurement activities constitute the Check phase. Raising concerns and investigations are also included here.

The last phase is about refining the activities of the previous phases and continual improvement. Managing noncompliance, either prevention or correction, is part of this phase. Finally, ISO 37301 requires organizations to maintain documented information on compliance risk assessment, records of nonconformities, and investigations.

*2.3. Compliance Risk Assessment.* Every company that implements a compliance risk management program develops a self-developed process-based solution adapted to the needs and characteristics of the organization, reflecting regulatory and internal needs [2]. A compliance risk assessment program can be a helpful management tool because companies can reduce the number and severity of compliance incidents and improve their business operations by better identifying compliance risks and managing behaviors [39].

Standardized risk prevention requires identifying and quantifying risk based on risk assessment methodologies. Risk identification usually describes the following characteristics of a risk, its nature, source, and impact, for example, incident, business line, and regulatory outcome [40]. The risk matrix is a widely used risk assessment method in the banking sector that uses two rating factors, usually to estimate the “occurrence” and “severity” dimensions of risk incidents [2]. Kim et al. [41] analysed risk assessment standards and proposed a new method for identifying and evaluating financial information security risks through correlation analysis between various security standards and requirements. Naheem’s [12] study concluded that risk assessment strategies remain largely reactive, leaving banks exposed to not realizing the risk by failing to conduct an assessment. The practical implications call for a more holistic, future-oriented approach from the bank’s perspective [12].

The so-called “compliance dilemma” is a collective term for conflicts over the exercise of compliance activities within a company. For example, a compliance dilemma is when a manager perceives a contradiction between a legitimate decision-making alternative and an alternative that fits the organization’s (e.g., financial) goals [42]. A study examining the minutes of the board meetings of Indian banks found that bank boards generally underinvest in risk and overinvest in regulation and compliance [43].

Organizations that aim for competitive advantage, organizational sustainability, and business success shall create a culture of compliance, a set of values, beliefs, and behaviors that create the norms that promote compliance. Compliance culture enhances such norms, attitudes, and work styles (i.e., accountability) that make compliant behavior possible and preferred and is the general basis for decision-making. The incentive structure and the consistency of formal risk management with actual behavior may support creating and developing a compliance culture [44].

Risk control and mitigation aim at reducing the likelihood of failure causes and their negative impact. The implementation of risk mitigation measures is prioritized and scheduled due to the availability of professional and financial resources. Banks use various control mechanisms

(like internal procedures, the “four eyes” principle, Chinese walls, and access rights) to decrease risks [2].

In practice, compliance risk management is heavily based on consultations with expert groups, while the reliability of these consultations is rarely validated. Failure Mode and Effect Analysis is a widely used risk management methodology in most industries, including the banking sector. Instead of a standard risk matrix [2], FMEA applies three rating factors (severity, occurrence, and detectability) for risk assessment. The FMEA aims to assess failure modes related to a process or product and then reduce the risks via risk mitigation action plans [45]. The Partial Risk Map (PRISM) methodology is a novel risk assessment technique that closely resembles the risk assessment process of the FMEA. The basics of the PRISM method are described [9], and potential development areas are also addressed related to the methodology and application fields [46, 47]. Since compliance risk assessment is a complex evaluation and ranking process, MCDM methods are relevant methodological solutions for modeling complexity in the decision-making process. The possible classification of MCDM universe is presented by Cinelli et al. [48], and there are other significant works comparing different MCDM methods. In the work of Valipour et al. [49], seven different MCDM methods are applied for PPP project assessment, including pairwise comparison techniques and outranking methods in some cases combined with fuzzy logic. Analytic Hierarchy Process (AHP) is combined with Multi-Choice Goal Programming (MCGP) to project selection and resource allocation in risk-based internal audit planning [50]. For Risk Priority Number (RPN) calculation, Djenadic et al. [51] combined AHP with TOPSIS in a fuzzy environment in order to model uncertainty among expert choices.

Since pairwise comparison techniques are applied in the literature for factor weight calculation, the primary identified development direction of the PRISM method is based on pairwise comparison methods. Thus, the risk assessment process can be opened for subjective weightings. Another advantage of the combination with pairwise comparison methods is that the consistency of the experts can be tested [50–52], while this option is not applicable in the original PRISM method. This shortcoming of the PRISM method can be vital in bank compliance risk assessment; thus, combining the method with pairwise comparison techniques is highly suggested.

Applying pairwise comparison methods is a traditional basis for assessing and evaluating complex systems [38, 53]. Typical solutions of pairwise comparisons are the Guilford method [54], where only the preferences between the elements of pairs are determined, and the methodology of the AHP, where the strength of the preferences is also set [55]. Best Worst Method (BWM) is a preferred pairwise comparison technique if a large number of items should be compared while also setting the strength of preferences [56]. All methods give feedback on the consistency level of the experts [52, 56–58]. The Guilford method can be advised as a primary pairwise comparison technique of compliance risk assessment. Since the compliance risk assessment used to be a significantly subjective process due to the complex nature

of bank compliance, preference determination is also subjective. Setting preferences' strengths can cause an uncontrolled level of subjectivity in the assessment.

Total elimination of the risk of noncompliance is impossible; however, residual risks must be controlled and monitored. The risk-based approach to verifying compliance with a sound compliance culture can deliver significant cost savings while leading to better business management and greater flexibility in response to changes in the business context [59]. Naheem's [60] study supports the argument for integrating social corporate responsibility and anti-money laundering compliance, in contrast to the current practice of profit and business being seen as separate rather than integral to regulation and control. Authorities increasingly rely on risk assessment techniques to increase their regulatory effectiveness, for example, by increasing supervision of companies with high-risk profiles, assuming high levels of disclosure [61].

Compliance risk assessment has complex methodological options, and it is unique to each organization. Therefore, the consistency check of the experts is an advantage of a risk assessment technique, especially when the assessment is complex, just like in the case of bank compliance. The proposed pairwise comparison-based Partial Risk Map method is described in the following section.

### 3. Methods

The process flow of the proposed extended PRISM method is introduced in detail in Figure 2. The detailed formal description of the proposed method follows the visual process flow.

The first step is forming a set of comparable elements, while the focus group of the experts can also be established. The second step is creating the pairwise comparison sheets based on Ross's optimal order [62, 63] separately to the occurrence, severity, and detection rating factors.

Let  $n$  indicate the number of incidents. Thus,  $p$  number of pairs can be formed based on equation

$$p = \frac{n(n-1)}{2}. \quad (1)$$

The third step is setting the experts' priorities and checking the experts' consistency. The level of consistency can be calculated based on equation

$$K = 1 - \frac{d}{d_{\max}}. \quad (2)$$

In equations (2)–(4),  $d_{\max}$  represents the highest possible number of inconsistent triads in a pattern. In the case of odd  $n$ :

$$d_{\max} = \frac{n^3 - n}{24}. \quad (3)$$

In the case of even  $n$ , the equation of  $d_{\max}$  is the following:

$$d_{\max} = \frac{n^3 - 4n}{24}. \quad (4)$$

In equations (2) and (5),  $d$  represents the number of inconsistent triads in a certain paired comparison pattern, and it is calculated using the following formula:

$$d = \frac{n(n-1)(2n-1)}{12} - \frac{\sum a_i}{2}, \quad (5)$$

where  $a_i$  indicates how often a specific  $i$  element was preferred to the other elements.

Based on a chi-square distribution significance test, whether a certain  $d$  number of inconsistent triads indicates a random or systematic inconsistency in a pairwise comparison pattern can be identified. For calculating the degree of freedom (DF) for the chi-square distribution, equation (6) can be used:

$$DF = \frac{n(n-1)(n-2)}{(n-4)^2}. \quad (6)$$

Equation (7) is applied to calculate the chi-square value:

$$\chi^2 = \frac{8}{(n-4)} \left\{ \frac{1}{4} \left( \frac{3}{n} \right) - d + \frac{1}{2} \right\} + DF. \quad (7)$$

In the case of systematic inconsistency, the individual assessment results cannot be used for further calculations.

As for the fourth step, a similarity check of the ranks of the incidents related to each consistent pattern should be executed. Based on testing the similarity, it can be decided whether the patterns can be aggregated—forming a group assessment result—or not. In the case of two ranks, rank correlation analysis can be applied to check the level of similarity. In the case of more than two ranks, aggregation can be executed or rejected based on the result of rank concordance analysis. This paper's similarity analysis is based on the calculation of Spearman's rho [64] in the case of two rankings and the calculation of Kendall's  $W$  [65] in the case of more than two rankings.

The value of Spearman's rank correlation coefficient is between  $-1$  and  $1$ . If the ranks are the same, Spearman's rho will be  $1$ . If the ranks are opposite, Spearman's rho will be  $-1$ . If the ranks are independent, Spearman's rho will be  $0$ . The value of Kendall's  $W$  coefficient is between  $0$  and  $1$ . In the case of the same ranks, the value of  $W$  is  $1$ . If the ranks are opposite, the coefficient will be equal to  $0$ . A 5% significance level is offered to test rank similarity in the case of both coefficients.

If the ranks are similar, the results of the individual assessments can be aggregated in the fifth step of the process. After the aggregation, it can be calculated how often a specific  $i$  element was preferred to the other elements in the aggregated pattern. Let  $c_i$  indicate the number of preferences in the aggregate matrix. Then, the  $p_c$  values can be calculated based on equation (8), where  $k$  is the number of consistent experts.

$$p_c = \frac{c_i + (k/2)}{nk}. \quad (8)$$



FIGURE 2: The steps of the proposed method.

Since the Guilford method ranks the comparable elements, it is necessary to introduce two theoretical variables representing the possible highest ( $C_1$ ) and lowest ( $C_2$ ) values of  $c_i$ . Based on equations (9) and (10), the value of  $C_1$  and  $C_2$  can be calculated.

$$c_{C1} = (n-1)k, \tag{9}$$

$$c_{C2} = (n-1)0 = 0. \tag{10}$$

The results of the Guilford method are projected to an interval scale by applying  $C_1$  and  $C_2$  values. Let  $u$  indicate the inverse normalized value of  $p_c$ . Linear transformation can transform  $u$  values to a selected scale [54, 58].

Since the values of occurrence, severity, and detection factors can be calculated related to each incident, as for the sixth step, the PRISM patterns of the incidents can also be set (see Figure 3). Since the PRISM methodology calculates the aggregate values of the paired rating factor values of an incident, denote  $p(m) = p(o, s, d) = (o \otimes s, o \otimes d, d \otimes s)$  as the PRISM pattern of incident  $m$ .

In the seventh step, the PRISM number of a particular incident can be calculated by selecting the maximal value of the three aggregates of  $p(m)$ . To test the validity of the

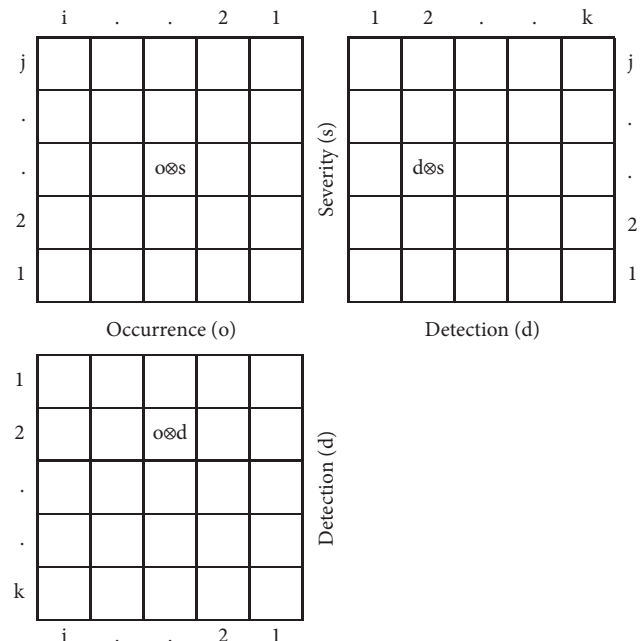


FIGURE 3: The PRISM pattern of an incident.

results, multi-assessment is performed, applying different threshold lines (linear, convex, and concave) in the submatrices of the PRISM. Equations (11)–(13) are applied in this study based on [66].

$$A(m) = \max(o + s, o + d, d + s), \quad (11)$$

$$M(m) = \max(o \cdot s, o \cdot d, d \cdot s), \quad (12)$$

$$S(m) = \max(o^2 + s^2, o^2 + d^2, d^2 + s^2), \quad (13)$$

where  $A(m)$  function results in linear,  $M(m)$  results in convex, and  $S(m)$  results in concave threshold lines from the perspective of the center of the PRISM [66].

In the eighth step, the individual and aggregated prioritization of the incidents can be executed based on the PRISM numbers. Applying  $A(m)$ ,  $M(m)$ , and  $S(m)$  functions, the similarity of the same expert rankings can be tested, providing feedback on the validity of the assessment. In addition, outlier experts can be identified by testing the similarity of the aggregated ranking and the individual rankings. Both tests strengthen the proposed method's reliability, which is necessary for the subjective assessment of complex phenomena.

Based on the result of the prioritization, further risk reduction actions can be planned and launched in the ninth step.

#### 4. Case Study

In 2021, a risk assessment workshop was launched in the compliance management directorate of one of the largest Central and Eastern European banks. After collecting bank branch-related compliance incidents, a focus group of the three top compliance experts was established. The focus group members had more than ten years of experience in the compliance management field in the commercial bank sector. This study presents the pairwise comparisons of six randomly selected incidents.

The experts assessed the cases (see Table 1) based on Guilford's pairwise comparison method. The assessment was executed three times since the cases had to be assessed based on the occurrence, severity, and detection factor. The results are given in Appendix A. Based on the Chi-Square statistic, if there are more than two inconsistent triads in a pattern ( $d > 2$ ), the decision maker is inconsistent at a 0.05 significance level. Hence, the result of the consistency evaluation of the experts showed that Expert 1 and Expert 2 were consistent in the occurrence, severity, and detection-based comparisons. In contrast, Expert 3 was consistent only in the severity-based comparison. The results of the consistency tests are given in Table 2.

The similarity test of the ranks can be executed after the consistency test. In the case of the severity factor, all the experts were consistent (Kendall's  $W$  is calculated). In contrast, two experts can be involved in the case of the occurrence and the detection factors (Spearman's rho is calculated). Kendall's  $W$  is 0.947 at a 0.014 significance level in the case of the severity factor (all experts were consistent).

In the case of the occurrence factor, Spearman's rho is 0.829 at 0.042 significance level (only Expert 1 and Expert 2 were consistent). In the case of the detection factor, Spearman's rho is 0.883 at a 0.02 significance level (Expert 1 and Expert 2 were consistent).

Since the patterns are significantly similar, the aggregation by factors can be executed. The results of the aggregation are given in Appendix B.

Based on the scale values of the occurrence, severity, and detection factors, the PRISM patterns of the incidents can be visualized (see Figure 4). The PRISM numbers are also visible in Figure 4 based on the maximal values of each case (see Table 3). The PRISM numbers are indicated with a dashed outline and darker color (see Figure 4) and bold numbers (see Table 3).

In this case study,  $A(m)$ ,  $M(m)$ , and  $S(m)$  functions give the same rankings related to the aggregated results, although the rankings could differ by function. In the case of Expert 1, different functions result in different rankings, while in the case of Expert 2, the rankings by different functions are the same. Expert 3 has no consistent occurrence and detection-related pairwise comparison results. Thus, for Expert 3, the PRISM cannot be constructed because of two missing factors.

Testing the impact of each expert's rankings on the aggregated ranking is optional, but it can highlight significant results of the entire analysis. The test can also help identify the best-fitting and outlier experts. Based on the data in Appendix A, the PRISM rankings of Expert 1 and Expert 2 can be calculated. After that, rank correlation analysis can be performed to describe the correlations between each expert's ranking and the aggregated ranking. The higher the correlation coefficient value, the better the fit to the aggregated rankings. If the significance level of the correlation coefficient is lower than 0.05, the expert will be marked as an outlier expert. Spearman's rho is applied for the calculation.

The rankings of each expert related to the  $A(m)$ ,  $M(m)$ , and  $S(m)$  functions are visible (see Table 4), as well as the aggregated rankings. Since the aggregated rankings and Expert 2's rankings have no differences by the PRISM functions, these rankings are placed in the table only once.

Since  $A(m)$ ,  $M(m)$ , and  $S(m)$  functions resulted in different rankings in the case of Expert 1, it is necessary to test the similarity of the rankings of Expert 1. For testing the similarity, Spearman's rho is calculated (see Table 5).

The correlation coefficients are high in all the comparisons, and the significance level was higher than 0.05. Thus, there is no outlier expert in the analysis, and the rankings of Expert 1 are similar. Without applying further non-parametric tests (Kendall's  $W$ ), it can be identified that  $S(m)$  function gives the most similar expert rankings.

Based on the results, C6 has the highest relative partial risk in the analysis. Thus, it is the riskiest incident. Since this top partial risk can be identified in the occurrence vs. detection submatrix, the possible optimal development or risk mitigation strategy is to decrease the occurrence level or increase the detectability level of the incident.

As all the consistent experts agreed, C5 is the least risky incident. There are slight changes in the ranks of C1, C2, C3,

TABLE 1: Randomly selected risks involved in the risk assessment.

Case	Function/process step	Potential failure	Potential effects of failure
C1	Cash withdrawal in a bank branch	A young person accompanies the elderly customer	Client losing wealth
C2	Looking into client accounts	Checking acquaintance's account after a phone call on business mobile	Protocol violation
C3	Replying to a customer inquiry about account abuse	Customer misinformation, and lack of reporting to bank security	Client losing wealth, security incident
C4	Cash withdrawal, account closing	The legal representative of a minor client withdraws the total amount and closes the account	Minor client losing wealth
C5	New account opening	A bank clerk opening a new account for a family member	Conflict of interest, protocol violation
C6	Offering travel insurance	Lack of reporting foreign card use	Credit card abuse



TABLE 2: Results of the consistency test.

Factor	Index	Expert 1	Expert 2	Expert 3
O	<i>d</i>	0	0	4
	<i>K</i>	100%	100%	50%
S	<i>d</i>	0	0	1
	<i>K</i>	100%	100%	87.5%
D	<i>d</i>	0	2	3
	<i>K</i>	100%	75%	62.5%

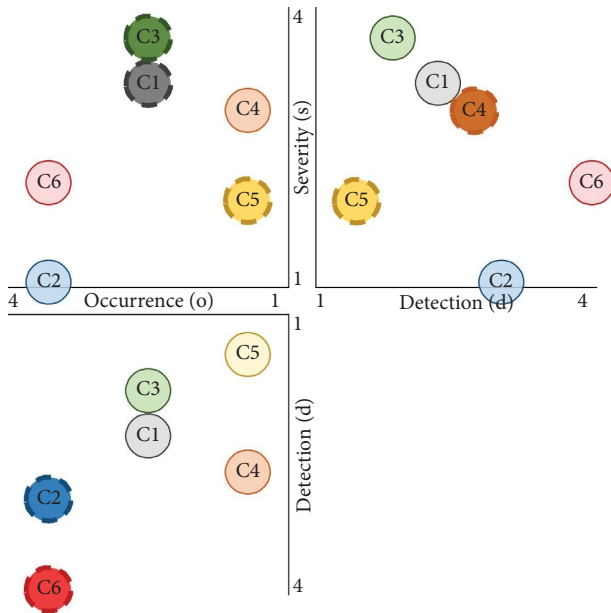


FIGURE 4: The visualization of the PRISM patterns and the PRISM numbers of the incidents.

TABLE 3: PRISM numbers based on the aggregated values in Appendix B.

	Case	<i>o-s</i>	<i>o-d</i>	<i>d-s</i>	Max	Rank
<i>A (m)</i>	C1	<b>8.1</b>	5.7	7.3	8.1	4
	C2	3.5	<b>10.5</b>	3.0	10.5	2
	C3	<b>9.2</b>	4.4	6.5	9.2	3
	C4	4.2	4.0	<b>7.9</b>	7.9	5
	C5	<b>2.8</b>	2.1	<b>2.8</b>	2.8	6
	C6	7.5	<b>14.2</b>	8.5	14.2	1
<i>M (m)</i>	C1	5.7	4.8	5.5	5.7	4
	C2	4.5	<b>6.5</b>	4.0	6.5	2
	C3	<b>6.2</b>	4.3	5.4	6.2	3
	C4	4.3	4.2	<b>5.6</b>	5.6	5
	C5	<b>3.4</b>	2.9	<b>3.4</b>	3.4	6
	C6	5.7	<b>7.6</b>	6.1	7.6	1
<i>S (m)</i>	C1	<b>16.7</b>	11.4	15.6	16.7	4
	C2	13.6	<b>21.4</b>	9.8	21.4	2
	C3	<b>19.8</b>	9.4	16.7	19.8	3
	C4	10.4	9.5	<b>15.8</b>	15.8	5
	C5	<b>5.9</b>	4.2	<b>5.9</b>	5.9	6
	C6	17.1	<b>28.6</b>	20.5	28.6	1

The bold values are highlighting the PRISM numbers.

TABLE 4: Rankings by experts and functions.

Cases	Expert 1			Expert 2	Aggregated ranking
	<i>A (m)</i>	<i>M (m)</i>	<i>S (m)</i>		
C1	4	5	4	4	4
C2	3	3	3	2	2
C3	2	2	2	3	3
C4	4	4	5	5	5
C5	5	6	6	6	6
C6	1	1	1	1	1

TABLE 5: Correlation coefficients of the similarity tests.

	Expert 1		Expert 2	Aggregated ranking
	<i>M (m)</i>	<i>S (m)</i>		
Expert 1 ( <i>A (m)</i> )	0.986	0.986	0.928	0.928
Expert 1 ( <i>M (m)</i> )		0.943	0.886	0.886
Expert 1 ( <i>S (m)</i> )			0.943	0.943
Expert 2				1.000

and C4 applying different functions, but as the analyses showed, these changes are moderate.

Since only significantly consistent experts were involved in the aggregated assessment and the individual assessments were similar, it can be concluded that the assessment is based on adequate knowledge, and the results are reliable.

## 5. Discussion and Managerial Implications

**5.1. Discussion.** A risk-based approach in compliance management is best practice internationally [37, 59], and reducing risks requires company-wide collaboration. However, breaking down principles and theories into methods and techniques is challenging and highly dependent on industry, size, and strategy. Therefore, compliance risk management is always unique for the organization. Understanding the legal and business context is critical in planning and operating a compliance management system [31, 36].

Effective compliance programs identify and control risks that could lead to financial and reputational loss or legal consequences [67]. Many indicators used to monitor compliance risks are also used to monitor operational risks. Therefore, an integrated operational and noncompliance risk framework can lead to practical solutions and reduced costs [68]. Appropriate techniques for the risk-based approach are listed in Annex B of IEC 31010:2019, which contains 31 risk assessment techniques, including Failure Mode and Effect Analysis (FMEA) [69]. In reality, methods and techniques are often determined by the practices and preferences of stakeholders and parent companies [70]. Risk assessment is helpful in the design phase of new products, services, or processes and for actual business processes. In practice, compliance risk management is heavily based on

consultations with expert groups, while the reliability of these consultations is rarely validated.

The risk matrix is a widely used risk assessment method in the banking sector, which has several weak points. First, the risk matrix is created along only two dimensions. The “probability” dimension is essentially the same as the “occurrence” factor of the FMEA. In contrast, “impact” is essentially the “severity” of the consequences of a failure mode in the FMEA. The issue of detectability is typically left out of the traditional risk matrix. In some cases, users interpret it as part of the probability, i.e., it is confused with the simple frequency of occurrence in the probability dimension. In addition to the advantages of the detectability dimension, with the help of the proposed pairwise comparison-based PRISM method, experts can check the consistency of individual decisions and identify outliers.

This study focuses on the assessment of partial or hidden risks. According to [71], knowledge discovery based on MCDM methods is a widely emerging field of the risk management of financial institutions. Combining the PRISM method with Guilford’s pairwise comparison is an alternative to the original PRISM method, which uses deterministic scales for assessing the FMEA factors. When assessors compare the alternatives in pairs to judge which is preferred in light of a rating factor (like severity), the method allows testing the decisions’ inconsistency. The consistency testing of expert evaluations is an advantage in highly complex matters. On the one hand, the main result of the risk assessment is the aggregated ranking of risks. On the other hand, outlier experts can be identified based on testing the impact of individual expert rankings on the aggregated ranking.

Based on the prioritization of the incidents by PRISM numbers, possible risk mitigation or reduction actions can be planned and launched. However, organizations should reassess risks periodically. In addition, reassessment is needed when new activities are launched and significant external changes (like a pandemic or war situation) or changes in the organizational structure (like mergers and acquisitions) happen.

On the one hand, risk management aims to control and reduce the likelihood of errors in compliance and the scope of their negative consequences [2]. On the other hand, actions may aim at improving the detectability of issues by designing controls within the processes. A common pitfall of compliance risk assessment is when management has already decided, without understanding the underlying causes, which risk they want to address in the next period. In the case of forced solutions, risk mitigation is artificially prioritized.

*5.2. Managerial Implications in Light of the Proposed Methodological Process and the Shortcomings of the Bank’s Practice.* The compliance risk assessment process is qualitative and based on historical data if data are available. The group assessment is based on discussion; no individual assessments are performed. The bank uses the risk matrix technique for risk assessment practices related to noncompliance events.

Since many banks have the same main compliance management processes, practical observations can be made based on comparing the bank’s compliance risk assessment process and the proposed process. The risk matrix determines the degree of risk based on predefined scales to assess the probability of occurrence and severity of impact. Figure 5 shows the structure of the matrix.

Determining the likelihood of the issue occurring describes the possibility in the foreseeable future. The probability of noncompliance events or their causes can fall into four categories: unlikely (happens once in more than five years), possible (happens every 3–5 years), likely (happens every 1–3 years), and very likely (occurs within 12 months). Often, historical data analysis is included in the estimation of incident occurrence.

The severity of noncompliance events is classified as follows: low (no or little financial loss, no reputational impact), medium (small financial loss, slight negative regional-level reputational impact), significant (significant financial loss or regional reputational impact, legal consequences), and severe (severe financial or legal consequences or global reputational impact).

The overall compliance risk rating can be aggregated into four categories: minor, moderate, significant, and critical. The risk rating is represented in four colors (green, yellow, orange, and red), where the yellow and orange categories are warnings and encourage corrective measures. Some corrective action is required for risks at any level over the minor. Based on the risk matrix, experts can visualize the accumulated risk of certain operations or departments.

The first problem of the risk matrix technique is that the risk matrix does not involve the ease of detection of failures and causes of noncompliance. Obviously, if a failure is harder to detect, it will pose more risk on the operations. PRISM and any FMEA-based methods dealing with severity, occurrence, and detection rating factors provide a basic solution for this practice.

The second major problem with the practice of bank is that applying predefined scales for the assessment does not allow for testing the consistency of the experts. The combination of the PRISM method with pairwise comparison techniques solves this problem. Since in the practice of the bank only group assessment is performed, the control possibilities of any individual expert results are unfeasible. Thus, important information related to similarity measure testing cannot be provided, for example, outlier experts cannot be identified. The proposed risk assessment process is based on the aggregation of individual results, so the previously mentioned problem of the bank’s process can be solved. In the bank practice, there are only four outputs as for the result of the risk assessment (minor, moderate, significant, and critical), so in case of many assessable issues, many items will have the same output value. Thus, in the case of scarce resources, there is no support information on which issue having the same output value should be mitigated first. Applying the proposed PRISM method, the final ranking will be more detailed than that in the bank practice. Although only a few problems were mentioned, hopefully, these can create motivation for the compliance experts of the

Severity	serious	Significant	Significant	Critical	Critical
	high	Moderate	Significant	Significant	Critical
	medium	Moderate	Moderate	Moderate	Significant
	low	Minor	Minor	Minor	Minor
		unlikely	possible	likely	very likely
		Occurrence			

FIGURE 5: Risk matrix in the practice of the compliance office.

bank (and in other banks where the characteristics of the risk assessment processes are quite similar) to conceive developments in the compliance management system.

## 6. Conclusions

This article presented a new compliance risk assessment method based on a commercial banking case study. Compliance management refers to the processes and controls that ensure that a company and its employees conduct their business legally and ethically. ISO 37301:2021 is the contextual background where the risk approach to compliance management is the foundation. In practice, the most popular risk assessment methods are combined with Multi-Criteria Decision-Making methods to describe complex phenomena more accurately. The PRISM method based on pairwise comparisons aligns with this trend.

The new method highlights that pairwise comparisons can provide an opportunity to compare the risk rankings of compliance experts and their consistency with aggregate rankings. In addition, this method allows organizations to identify inconsistent and outlier experts. Significantly different assessments may include valuable insights into a particular phenomenon or differing interpretations of complex issues.

As a limitation, this case study was presented with only a small incident sample, but the results of statistical methodologies are valid. The agreement between the three organizational experts is significant. Furthermore, the case study did not examine whether the professional experience or the time spent at the particular bank was related to the rankings resulting from the evaluation.

A methodological limitation of this work is that the uncertainty related to the experts' opinions on the pairwise comparison process cannot be modeled well, since the proposed method applies binary output indicating the preferences. Instead of AHP and BMW methods which can

be fuzzified well, in the case of the proposed method, fuzzification seems to be cumbersome. The Guilford method has almost the same limitation as the AHP, that is, the number of comparable items is quite low, according to human brain capacity. In the case of many comparable elements, the PRISM method should be integrated with BMW instead of binary techniques or AHP.

Future research could focus on decision-making and how group assessment techniques, such as the traditional FMEA, can be combined with individual assessment techniques. Another possible research direction is a methodological extension, namely, the combination of AHP or BWM and PRISM when the relationship between two risks (incidents) and the strength of the preferences are also included in the evaluations. Furthermore, since fuzzification is a developing research field besides the MCDM methods [72] in the description of complex systems, the fuzzy-based hybrid development of the PRISM method can also be a possible future development direction. Fuzzy logic is efficient for handling uncertain and imprecise knowledge, which is sometimes the case in the bank compliance area. Similarly, since risk factor estimations are based on previous observations and experience, the consideration of the uncertainty associated with these observations [73] and the risk of decision errors [74] is another route to extend the proposed method. Finally, future research could investigate the human element in compliance risk management, from individual characteristics that affect compliance dilemmas at work to compliance culture.

## Data Availability

The data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work has been implemented by the TKP2020-NKA-10 project with the support provided by the Ministry for Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the 2020 Thematic Excellence Programme funding scheme.

## Supplementary Materials

Appendix A: the individual results of the pairwise comparisons. Appendix B: the aggregated results including the sufficiently consistent individual results. (*Supplementary Materials*)

## References

- [1] COSO, *Compliance Risk Management: Applying the COSO ERM Framework* COSO, Washington, WA, USA, 2020.

- [2] E. Losiewicz-Dniestrzanska, "Monitoring of compliance risk in the bank," *Procedia Economics and Finance*, vol. 26, pp. 800–805, 2015.
- [3] E. Losiewicz-Dniestrzanska and A. Nosowski, "The risk of non-compliance in the context of a banking business model," *New Trends and Issues Proceedings on Humanities and Social Sciences*, vol. 3, no. 4, pp. 198–207, 2017.
- [4] O. S. Bezrodna, "Strategic risk of a bank: assessment proposals and interrelation with the compliance risk," *Business Inform*, vol. 12, no. 503, pp. 317–324, 2019.
- [5] B. Makowicz, *Compliance W Przedsiębiorstwie*, Oficyna Wolters Kluwer Business, Warszawa, Poland, 2011.
- [6] P. Benedek, "Compliance management – a new response to legal and business challenges," *Acta Polytechnica Hungarica*, vol. 9, no. 3, pp. 135–148, 2012.
- [7] M. Hashmi, G. Governatori, H. P. Lam, and M. T. Wynn, "Are we done with business process compliance: state of the art and challenges ahead," *Knowledge and Information Systems*, vol. 57, no. 1, pp. 79–133, 2018.
- [8] H. C. Liu, X. Q. Chen, C. Y. Duan, and Y. M. Wang, "Failure mode and effect analysis using multi-criteria decision making methods: a systematic literature review," *Computers & Industrial Engineering*, vol. 135, pp. 881–897, 2019.
- [9] F. Bognár and P. Benedek, "A novel risk assessment methodology: a case study of the PRISM methodology in a compliance management sensitive sector," *Acta Polytechnica Hungarica*, vol. 18, no. 7, pp. 89–108, 2021.
- [10] L. Ouyang, Y. Che, L. Yan, and C. Park, "Multiple perspectives on analyzing risk factors in FMEA," *Computers in Industry*, vol. 141, Article ID 103712, 2022.
- [11] D. M. Salvioni, F. Gennari, and L. Bosetti, "Global Responsibility and Risks of Compliance Failure in Emerging Markets," in *Risk Management in Emerging Markets*, S. Boubaker, B. Buchanan, and D. K. Nguyen, Eds., Emerald Group Publishing Limited, Bingley, UK, 2016.
- [12] M. A. Naheem, "Anti-money laundering/trade-based money laundering risk assessment strategies – action or re-action focused?" *Journal of Money Laundering Control*, vol. 22, no. 4, pp. 721–733, 2019.
- [13] C. Eckert and N. Gatzert, "The impact of spillover effects from operational risk events: a model from a portfolio perspective," *The Journal of Risk Finance*, vol. 20, no. 2, pp. 176–200, 2019.
- [14] R. Boffey and G. N. Robson, "Bank credit risk management," *Managerial Finance*, vol. 21, no. 1, pp. 66–78, 1995.
- [15] Q. K. Nguyen and V. C. Dang, "Does the country's institutional quality enhance the role of risk governance in preventing bank risk?" *Applied Economics Letters*, vol. 30, no. 6, pp. 850–853, 2022.
- [16] A. Demirgüç-Kunt, E. Detragiache, and T. Tressel, "Banking on the principles: compliance with Basel core principles and bank soundness," *Journal of Financial Intermediation*, vol. 17, no. 4, pp. 511–542, 2008.
- [17] A. Demirgüç-Kunt and E. Detragiache, "Cross-Country Empirical Studies of Systemic Bank Distress: A Survey," *National Institute Economic Review*, vol. 192, pp. 68–83, 2005.
- [18] J. R. Barth, G. Caprio, and R. Levine, "Bank regulation and supervision: what works best?" *Journal of Financial Intermediation*, vol. 13, no. 2, pp. 205–248, 2004.
- [19] S. Tran, D. Nguyen, K. Nguyen, and L. Nguyen, "Credit booms and bank risk in Southeast Asian countries: does credit information sharing matter?" *Asia-Pacific Journal of Business Administration*, 2022.
- [20] G. Birindelli and P. Ferretti, "Compliance function in Italian banks: organizational issues," *Journal of Financial Regulation and Compliance*, vol. 21, no. 3, pp. 217–240, 2013.
- [21] J. A. Conger, D. Finegold, and E. E. Lawler, "Appraising boardroom performance," *Harvard Business Review*, vol. 76, no. 1, pp. 136–148, 1998.
- [22] L. J. Abbott, S. Parker, and G. F. Peters, "Audit committee characteristics and restatements," *Auditing: A Journal of Practice & Theory*, vol. 23, no. 1, pp. 69–87, 2004.
- [23] B. Xie, W. N. Davidson, and P. J. DaDalt, "Earnings management and corporate governance: the role of the board and the audit committee," *Journal of Corporate Finance*, vol. 9, no. 3, pp. 295–316, 2003.
- [24] Q. K. Nguyen, "Oversight of bank risk-taking by audit committees and Sharia committees: conventional vs Islamic banks," *Heliyon*, vol. 7, no. 8, Article ID e07798, 2021.
- [25] Q. K. Nguyen, "Audit committee structure, institutional quality, and bank stability: evidence from ASEAN countries," *Finance Research Letters*, vol. 46, Article ID 102369, 2022.
- [26] O. Masood, H. Al Suwaidi, and P. Darshini Pun Thapa, "Credit risk management: a case differentiating Islamic and non-Islamic banks in UAE," *Qualitative Research in Financial Markets*, vol. 4, no. 2/3, pp. 197–205, 2012.
- [27] N. Alam and K. Boon Tang, "Risk-taking behaviour of Islamic banks: application of prospect theory," *Qualitative Research in Financial Markets*, vol. 4, no. 2/3, pp. 156–164, 2012.
- [28] M. A. Ashraf and A. Lahsasna, "Proposal for a new Shari'ah risk rating approach for Islamic banks," *ISRA International Journal of Islamic Finance*, vol. 9, no. 1, pp. 87–94, 2017.
- [29] R. Basiruddin and H. Ahmed, "Corporate governance and Shariah noncompliant risk in Islamic banks: evidence from southeast asia," *Corporate Governance: The International Journal of Business in Society*, vol. 20, no. 2, pp. 240–262, 2019.
- [30] A. R. Syaputri and Y. A. Nainggolan, "Does political connection affect sharia non-compliance risk? Evidence from Indonesian and Malaysian Islamic banks," *Journal of Sustainable Finance & Investment*, pp. 1–27, 2022.
- [31] ISO, *Compliance Management Systems - Requirements with Guidance for Use*, ISO, London, UK, 2021.
- [32] J. A. Petrick and J. F. Quinn, "The integrity capacity construct and moral progress in business," *Journal of Business Ethics*, vol. 23, no. 1, pp. 3–18, 2000.
- [33] C. J. Fombrun and M. Shanley, "What's in a name? Reputation building and corporate strategy," *Academy of Management Journal*, vol. 33, no. 2, pp. 233–258, 1990.
- [34] D. Koehn, "Integrity as a business asset," *Journal of Business Ethics*, vol. 58, no. 1-3, pp. 125–136, 2005.
- [35] L. Tourigny, W. L. Dougan, J. Washbush, and C. Clements, "Explaining executive integrity: governance, charisma, personality and agency," *Management Decision*, vol. 41, no. 10, pp. 1035–1049, 2003.
- [36] R. Hendra, "Comparative review of the latest concept in compliance management & the compliance management maturity models," *RSF Conference Series: Business, Management and Social Sciences*, vol. 1, no. 5, pp. 116–124, 2021.
- [37] F. Bezzina, S. Grima, and J. Mamo, "Risk management practices adopted by financial firms in Malta," *Managerial Finance*, vol. 40, no. 6, pp. 587–612, 2014.
- [38] A. Boros and C. Fogarassy, "Relationship between corporate sustainability and compliance with state-owned enterprises in central-europe: a case study from Hungary," *Sustainability*, vol. 11, no. 20, p. 5653, 2019.
- [39] S. Nicolas and P. V. May, "Building an effective compliance risk assessment programme for a financial institution,"

- Journal of Securities Operations & Custody*, vol. 9, no. 10, pp. 215–224, 2017.
- [40] AIRMIC, *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*, AIRMIC, London, UK, 2010.
- [41] A. C. Kim, S. M. Lee, and D. H. Lee, “Compliance risk assessment measures of financial information security using system dynamics,” *International Journal of Security and its Applications*, vol. 6, no. 4, pp. 191–200, 2012.
- [42] G. Gösswein, “Mediation als Weg aus dem Compliance-Dilemma,” *Die Mediation*, vol. 2, p. 42, 2017.
- [43] S. Agarwal, S. Kamath, K. Subramanian, and P. Tantri, “Board conduct in banks,” *Journal of Banking & Finance*, vol. 138, Article ID 106441, 2022.
- [44] T. Poppensieker, S. Schneider, and M. Thun, “Financial institutions and non-financial risk: learning from the corporate approach,” in *Non-Financial Risk Management: Emerging Stronger after Covid-19*, T. Kaiser, Ed., Risk Books, London, UK, 1st edition, 2021.
- [45] J. Huang, J. X. You, H. C. Liu, and M. S. Song, “Failure mode and effect analysis improvement: a systematic literature review and future research agenda,” *Reliability Engineering & System Safety*, vol. 199, Article ID 106885, 2020.
- [46] A. Forgács, J. Lukács, and R. Horváth, “The investigation of the applicability of fuzzy rule-based systems to predict economic decision-making,” *Acta Polytechnica Hungarica*, vol. 18, no. 11, pp. 97–115, 2021.
- [47] P. Rosenberger and J. Tick, “Multivariate optimization of PMBOK, version 6 project process relevance,” *Acta Polytechnica Hungarica*, vol. 18, no. 11, pp. 9–28, 2021.
- [48] M. Cinelli, M. Kadziński, G. Miebs, M. Gonzalez, and R. Słowiński, “Recommending multiple criteria decision analysis methods with a new taxonomy-based decision support system,” *European Journal of Operational Research*, vol. 302, no. 2, pp. 633–651, 2022.
- [49] A. Valipour, H. Sarvari, and J. Tamošaitiene, “Risk assessment in PPP projects by applying different MCDM methods and comparative results analysis,” *Administrative Sciences*, vol. 8, no. 4, p. 80, 2018.
- [50] X. Wang, T. Zhao, and C. T. Chang, “An integrated FAHP-MCGP approach to project selection and resource allocation in risk-based internal audit planning: a case study,” *Computers & Industrial Engineering*, vol. 152, Article ID 107012, 2021.
- [51] S. Djenadic, M. Tanasijevic, P. Jovancic, D. Ignjatovic, D. Petrovic, and U. Bugaric, “Risk evaluation: brief review and innovation model based on fuzzy logic and MCDM,” *Mathematics*, vol. 10, no. 5, p. 811, 2022.
- [52] L. Berényi and N. Deutsch, “Corporate social responsibility and business philosophies among Hungarian business students,” *Sustainability*, vol. 13, no. 17, p. 9914, 2021.
- [53] J. Kiss, Z. Kosztyán, A. Németh, and F. Bognár, “Matrix-based methods for planning and scheduling maintenance projects,” in *Invest on Visualization Proceedings of the 13th International DSM Conference*, S. D. Eppinger, M. Maurer, K. Eben, and U. Lindemann, Eds., pp. 421–434, Carl Hanser Verlag, München, Germany, 2011.
- [54] J. P. Guilford, “The method of paired comparisons as a psychometric method,” *Psychological Review*, vol. 35, no. 6, pp. 494–506, 1928.
- [55] R. W. Saaty, “The analytic hierarchy process—what it is and how it is used,” *Mathematical Modelling*, vol. 9, no. 3-5, pp. 161–176, 1987.
- [56] J. Rezaei, “Best-worst multi-criteria decision-making method,” *Omega*, vol. 53, pp. 49–57, 2015.
- [57] M. Braglia, “MAFMA: multi-attribute failure mode analysis,” *International Journal of Quality & Reliability Management*, vol. 17, no. 9, pp. 1017–1033, 2000.
- [58] A. Buzási and B. S. Jäger, “District-scale assessment of urban sustainability,” *Sustainable Cities and Society*, vol. 62, Article ID 102388, 2020.
- [59] D. Batchelor, “Risk-based compliance monitoring,” *Journal of Financial Regulation and Compliance*, vol. 7, no. 1, pp. 22–26, 1999.
- [60] M. A. Naheem, “HSBC Swiss bank accounts-AML compliance and money laundering implications,” *Journal of Financial Regulation and Compliance*, vol. 23, no. 3, pp. 285–297, 2015.
- [61] D. De Widt and L. Oats, “Risk assessment in a cooperative compliance context: a Dutch-UK comparison,” *British Tax Review*, no. 2, pp. 230–248, 2017.
- [62] R. T. Ross, “Discussion: optimal orders in the method of paired comparisons,” *Journal of Experimental Psychology*, vol. 25, no. 4, pp. 414–424, 1939.
- [63] W. G. Cloete, I. Cloete, and K. von Gadow, “An algorithm for presenting pairs in optimum orders,” *EDV in Medizin und Biologie*, vol. 19, no. 2-3, pp. 75–77, 1988.
- [64] C. Spearman, “The proof and measurement of association between two things,” *American Journal of Psychology*, vol. 15, no. 1, pp. 72–101, 1904.
- [65] M. G. Kendall, *Rank Correlation Methods*, Griffin, London, UK, 1970.
- [66] F. Bognár and C. Hegedűs, “Analysis and consequences on some aggregation functions of PRISM (partial risk Map) risk assessment method,” *Mathematics*, vol. 10, no. 5, p. 676, 2022.
- [67] SIA, “White paper on the role of compliance,” 2005, <https://www.sifma.org/wp-content/uploads/2017/08/2005RoleofComplianceWhitePaper.pdf>.
- [68] PWC, “Managing compliance and operational risk in the new environment,” 2013, <https://www.pwc.com/fsi>.
- [69] IEC, “Risk Management-Risk Assessment Techniques 31010: 2019,” 2019, <https://www.iso.org/standard/72140.html>.
- [70] P. Benedek, “Compliance management in services,” *PhD Thesis*, , 2019.
- [71] W. Wu, “Credit risk measurement, decision analysis, transformation and upgrading for financial big data,” *Complexity*, vol. 2022, Article ID 8942773, 8 pages, 2022.
- [72] M. Kelemen, V. Polishchuk, B. Gavurová et al., “Model of evaluation and selection of expert group members for smart cities, green transportation and mobility: from safe times to pandemic times,” *Mathematics*, vol. 9, no. 11, p. 1287, 2021.
- [73] C. Hegedűs and Z. T. Kosztyán, “The consideration of measurement uncertainty in forecast and maintenance related decisions,” *Problems of Management in the 21st Century*, vol. 1, pp. 46–59, 2011.
- [74] Z. T. Kosztyán, C. Hegedűs, and A. Katona, “Treating measurement uncertainty in industrial conformity control,” *Central European Journal of Operations Research*, vol. 25, no. 4, pp. 907–928, 2017.