Multi-Method Risk Assessment Process for Sustainable Business – A Compliance Research Follow-up Case Study

Ferenc Bognár, Petra Benedek

Department of Management and Business Economics, Budapest University of Technology and Economics Magyar tudósok körútja 2, H-1117 Budapest, Hungary; bognar.ferenc@gtk.bme.hu; benedek.petra@gtk.bme.hu

Abstract: Assessing and reducing compliance risks for competitiveness, business continuity, and organizational sustainability requires sound methodologies. This study aims to characterize a multi-method assessment process that can show the experts the complex assessment options. This paper presents three multidimensional assessment methods following a case study at a commercial bank. The decision-making patterns related to the experts and assessment methods can be identified. Based on the best fit of the patterns, a possible solution can be offered for designing actions to reduce the risk of noncompliance, providing guidance for improvement aligning with organizational objectives to increase business continuity and sustainability. The results of this study can serve as a methodological input for compliance risk assessment in banks and other organizations in highly regulated sectors.

Keywords: risk assessment; compliance risk; Risk Matrix; Failure Mode and Effect Analysis; FMEA; Partial Risk Map; PRISM

Introduction

Reputation, trust, reliability, and ethical behavior are as relevant issues as decades ago [1]. Partnerships and business cooperation are fundamentally based on mutual trust and commitment. Since business is embedded in the social structures (like the legal environment), companies need business models that provide good quality products to ensure competitiveness and are also sustainable from a social and environmental perspective [2]. Modern societies express expectations for sustainable development, which means becoming more sustainable with incremental development [3].

The United Nations' Sustainable Development Goals (SDG) promote sustainable economic growth, higher productivity, and technological innovation. As a result, companies increasingly reflect the SDGs in their business models and strategies,

integrating sustainability into core business [4]. As a result of intense legal pressure, preparing a sustainability report has become a legal obligation for large companies in the European Union [5]. This report makes sustainability a compliance issue. The European Commission has defined Key Performance Indicators with the legislation [6, 7].

The compliance function ensures legal compliance in a highly complex environment with various actors. Compliance means complying with and enforcing the legal regulations that apply to a company, including the owner's decisions. One of compliance management's main tasks is ensuring the coherence of external and internal regulations. In addition, building trust and confidence is the underlying premise of all compliance activities [8, 9].

As part of the organization's internal control system, corporate compliance is responsible for identifying and managing compliance risks at the organizational level. Therefore, the compliance department requires functional independence, strong senior management support, and a strong network of contacts. In addition, prioritizing compliance issues requires increased attention from management and compliance officers. This study facilitates the understanding of the risk assessment processes that contribute to decision-making and executive behavior.

Controls aim to ensure the orderly, economical, efficient, and effective management of assets and the proper fulfillment of reporting obligations. The "lines of defense" describe the internal control system developed based on EU legislation in the financial sector. New risks appearing because of technological advancement or other significant changes must be fully understood and regulated adequately by authorities [10]. In addition, the challenges of the past three years (such as rapid changes in customer expectations and pandemic measures) have forced many actors to rethink their business and risk models and contributed to the closer integration of risk management and operational management.

The banking sector is one of the most regulated industries, has a significant influence on the economy, and has considerable experience managing regulatory risks. Banks operate in a global environment with rapidly evolving national and international regulation and supervision (including measurement and quantification of operational risk) to ensure a well-functioning banking system and promote stability. Financial institutions have developed compliance frameworks, advanced approaches, and techniques. However, non-financial risks arising from operations (processes and systems) are similar to those outside the financial sector [11]. The changing regulation forces businesses to reassess risks, strategies and action plans to comply with legal requirements. Companies can better adapt to a changing environment by developing a practical approach to managing risks and strengthening overall flexibility.

This paper focuses on the importance of individual risk assessment, using more than one risk assessment method in a complex environment, and provides valuable insights into compliance risk assessment. The purpose of this paper is to present a

detailed, multi-method risk evaluation process. The paper is organized as follows. Section 1 presents the compliance risk assessment background of the study. Section 2 introduces the methodology and the empirical research, including the materials, while Section 3 presents the results. In Section 4, the results are discussed, highlighting managerial implications. Finally, the conclusions summarize this paper and propose directions for future research.

1 Compliance Risk Assessment

Compliance risks are various, conditional, and unique to each organization. Their assessment is a complex issue since experts can evaluate compliance risks on many terms from several perspectives. If risk assessment is carried out regularly, trends can provide information on strengths and areas to be developed.

As a compliance management system is growing past its initial phase, there is a shift of focus from mere compliance incident detection and reacting to incidents to preventing noncompliance and a proactive culture [12, 13].

Compliance risk assessment forms the basis for implementing compliance management systems and allocating appropriate resources and processes to address identified compliance risks [14].

The compliance risk assessment process has three well-distinguished steps: (1) identifying compliance obligations and related compliance risks, like permits, contractual relationships, corruption, fraud, and the industry or quality standards. Secondly, (2) analysis of the probability (likelihood of occurrence) and the consequences of noncompliance, like environmental damage, economic loss, damage to reputation, and administrative burdens. Finally, (3) risk evaluation includes ranking and prioritization of risks.

Risk identification is a systematic activity that reveals how compliance obligations manifest in activities, products, services, and other relevant aspects of operations (such as digital transformation). Identifying compliance risk involves identifying compliance resources and situations and creating a database of these. If there is outsourced activity (i.e., HR processes), the responsibility for compliance still lies with the outsourcing organization. Therefore, outsourced and third-party processes must also be examined for risk identification. In addition, changing circumstances (like pandemic or war situation) or organizational context (like mergers or entering new markets) triggers new risk identification.

Compliance risks are to be analyzed and evaluated regularly, at least yearly. Furthermore, even a single noncompliance event or a so-called "near miss" (or "close call"), when no negative consequence (like an interruption to operations) followed an incident, should trigger the reassessment process. Furthermore, the extent and level of compliance risk assessment should be proportionate to the

organization's context, size, and objectives. Appropriate techniques for the risk-based approach are listed in Annex B of IEC 31010:2019, containing 31 risk assessment techniques, including Failure Mode and Effect Analysis (FMEA) [15]. Finally, risk assessment is not a collection of static practices but should evolve considering external changes in the business environment [11].

Risk evaluation is the last step of the risk assessment process. The analysis is followed by ranking and prioritization of the compliance risks. FMEA, Risk Matrix and Partial Risk Map are examples of techniques that can serve as a basis for developing risk reduction strategies, action plans and allocating resources.

The primary motivation of this study is to characterize a multi-method assessment process, which can show experts the complex options for their compliance assessment work. Based on the proposed assessment process, decision-making patterns related to experts and assessment methods can be identified. Finally, based on the best fit of the patterns, a possible solution can be offered to design actions that reduce the risk of noncompliance. The research question of this paper is:

Which group assessment method (nominal group or focus group) gives the closest result to individual assessments in the compliance risk ranking process?

Two assumptions are examined in this paper.

Assumption 1. The aggregation of individual rankings shows closer results to individual rankings than discussion-based rankings. (A1)

Assumption 2. In the case of Risk Priority Number, the consensus level will be significantly higher than in the case of Risk Exposure and PRISM number. (A2)

2 Materials and Methods

Section 2.1 briefly introduces the applied risk assessment methodologies in the case study, just like Risk Matrix (RM), Failure Mode and Effects Analysis, and Partial Risk Map (PRISM). This section also briefly introduces the comparative analyses' statistical methods (Spearman's rho rank correlation and Kendall's W rank concordance coefficients). Finally, in Section 2.2, the risk assessment process flow and the characteristics of the data are presented.

2.1 Methods

Several risk assessment methods can be applied when the risk assessment process is based on multi-criteria. For example, according to the Basel Committee [16], the risk of noncompliance in the banking sector can be estimated through several criteria. Thus, applying multi-criteria risk assessment tools can be relevant in the ranking process of the case study. In this study, three significantly different risk assessment methods are applied systematically to analyze the presented cases.

These methods are the Risk Matrix [17], the Failure Mode and Effect Analysis [18], and the Partial Risk Map [19]. In the following, these methods and their applied parameters are interpreted briefly.

As visible in Figure 1, the applied risk assessment techniques have different evaluation structures. While RM is a one-time two-dimensional and FMEA is a one-time three-dimensional, PRISM is a three-time two-dimensional assessment methodology. While the assessment process of RM and FMEA applies only one assessment (based on 2 or 3 dimensions) [20, 21], PRISM applies three assessments (each based on two of the dimensions) [19]. The "severity of consequences" (*S*) dimension and the "probability of occurrence" (*O*) are typically involved in all three assessment techniques. In contrast, the "undetectability" (*D*) dimension is only applied by the FMEA [22] and PRISM methods [19]. The higher the value of *O*, *S*, and *D*, the higher the factor related to the risk of the incident. Please note that the lower the probability that a failure mode (faulty condition) is detected during regular operation, the higher the risk of non-detection.

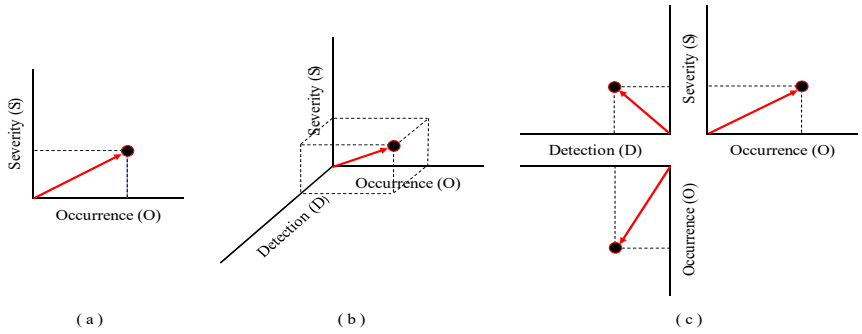

Figure 1
The structure of RM is shown by part (a), FMEA is shown by part (b), and PRISM is shown by part (c)

The role of aggregation functions is essential in the ranking result of the different methods. Based on [23], three typical aggregation functions are interpreted in these methods. The addition-based aggregation results linear, the multiplication-based aggregation results convex, while the sum-of-squares-based aggregation results in concave iso-risk lines for the ranking process. In the RM and PRISM methods, the addition and multiplication functions are used for the aggregation. In the case of FMEA, the multiplication function is often applied for aggregation [23, 24].

The purpose of applying the three methods is the same, to identify the possible or existing incidents by assessing the risks of the incidents. Once an incident is diagnosed as intolerably risky, risk reduction action is planned and launched to reduce the risk to a tolerable level [19]. The steps of evaluation and prioritization of risky incidents are different in the case of each method. Since these steps are not the focus of the study, a more profound introduction to different risk reduction processes of the different methods can be omitted. In the following, the definition of the incidents and the applied risk assessment functions are described.

Denote as m:=(o, s, d) an incident that has three risk characteristics: o probability of occurrence (O), s severity of consequences (S), and d undetectability (D). The characteristics have the following values, $o \in [1, 2, \cdots, i]$, $s \in [1, 2, \cdots, j]$ and $d \in [1, 2, \cdots, k]$. The scale lengths of o, s, and d are traditionally ten units in the case of FMEA, while four or five units in most cases of two-dimensional methods. Therefore, for all the incidents, the aggregate risk value can be calculated based on the values of the selected set of o, s, and d. The higher the value of the aggregation result, the higher the entire risk related to the incident.

As previously discussed, RM is a two-dimensional methodology built up to assess the risk of a particular process or object. The RM estimates the probability of occurrence (O) and the severity of consequences (S) of the specific process or object at the same time [20]. As previously noted, the addition aggregation function is applied in the case of RM and PRISM, while multiplication is used for the aggregation function of FMEA. Based on Equation 1, the Risk Exposure (RE) of a particular m incident can be calculated.

$$RE(m) = o + s \tag{1}$$

Since FMEA has one assessment vector and is a three-dimensional method, the indication of risk is compressed into an index called Risk Priority Number (RPN) [22]. Based on Equation 2, the RPN of a particular m incident can be calculated.

$$RPN(m) = o \times s \times d \tag{2}$$

The PRISM method applies a maximal value selection function over the three aggregation functions. The maximal value selection function can compress the risk level into the so-called PRISM number. Therefore, this method has three different partial risks related to the three two-dimensional assessments. Based on the PRISM number, the highest partial risks can be estimated [23]. Based on Equation 3, the PRISM number of a particular m incident can be calculated.

$$PRISM(m) = \max(o + s; o + d; s + d) \tag{3}$$

Based on the RE(m), RPN(m), and PRISM(m) values, the risk-based ranking of the incidents can be executed. Since the fundamental equations of the methods are different, the emerging rankings can also be different. Based on analyses of the differences between the rankings, information can be provided related to the topic of a research study. This paper uses the Spearman rank correlation analysis [25] to estimate the differences between paired rankings. Furthermore, the Kendall rank concordance analysis [26] is applied to estimate the differences between more than two rankings. Both analyses are often applied in focus-group-based qualitative assessments since the applied coefficients of the analyses can compare a minimal number (even just two) of records to each other [27]. A 5% significance level is applied in the analyses of both coefficients.

Spearman's rank correlation analysis is a statistical method usually applied to describe the strength and direction of a relationship between two variables. Spearman's rank correlation coefficient value ranges between -1 and 1. In the case of the same rankings, Spearman's rho equals 1. In the case of opposite rankings, Spearman's rho is -1. In the case of independent rankings, Spearman's rho is 0. In this study, Spearman's rank correlation coefficient was applied to analyze the pairwise similarities of the two rankings.

Kendall's rank concordance analysis is a non-parametric test. This statistic is often a prerequisite test before aggregating individual evaluations into group results. Based on the value of Kendall's W coefficient, the difference between at least two ranks can be characterized. The statistic is often used to compare different judgments to each other in social and economic sciences [26, 28]. The value of the coefficient is between 0 and 1. If the rankings are the same, the value of the coefficient is 1. If the rankings are the opposites, the coefficient is 0. The coefficient is generally used to interpret the agreement level of several judges. In the case of low coefficient values, the ranks are regarded as random, so different judgments cannot be aggregated.

2.2 Materials

In this subsection, materials are presented briefly, corresponding to the steps of the risk assessment process shown in Figure 2. Results from previous studies are also presented, as some serve as a relevant input for this study. The proposed risk assessment process consists of nine steps. From step 1 to step 4, the aim is on the details of group formation and assessment characteristics. Then, in step 5, the data validation process is performed. These five steps and their results are the subjects of previous studies [19, 27]. A brief description of the steps can be found in the following paragraphs.

In steps 1 and 2, case collection and expert selection are the focus. The assessment was launched at one of the top 5 largest Central and Eastern European commercial banks [19, 27]. Many possible compliance risks were described and presented by the bank. All the cases were related to the bank branch administration processes and focused on the characteristics of a possible non-compliant decision of the bank administrators. Any risk-taking behavior can open up additional opportunities for employee wrongdoing. Six risks were randomly selected for the process interpretation and results of the case study [19, 27]. The delegated compliance experts of the bank had at least ten years of experience in the field and were employed in the bank's headquarters. Two moderators also participated in the work of the focus group. The experts performed the assessment based on the *O*, *S*, and *D* dimensions, with four-four different factor values presented in [27].

In step 3, the focus group members had to assess the compliance cases individually [27]. Then in step 4, the group-decision assessment was delivered, including all the focus group members [19].

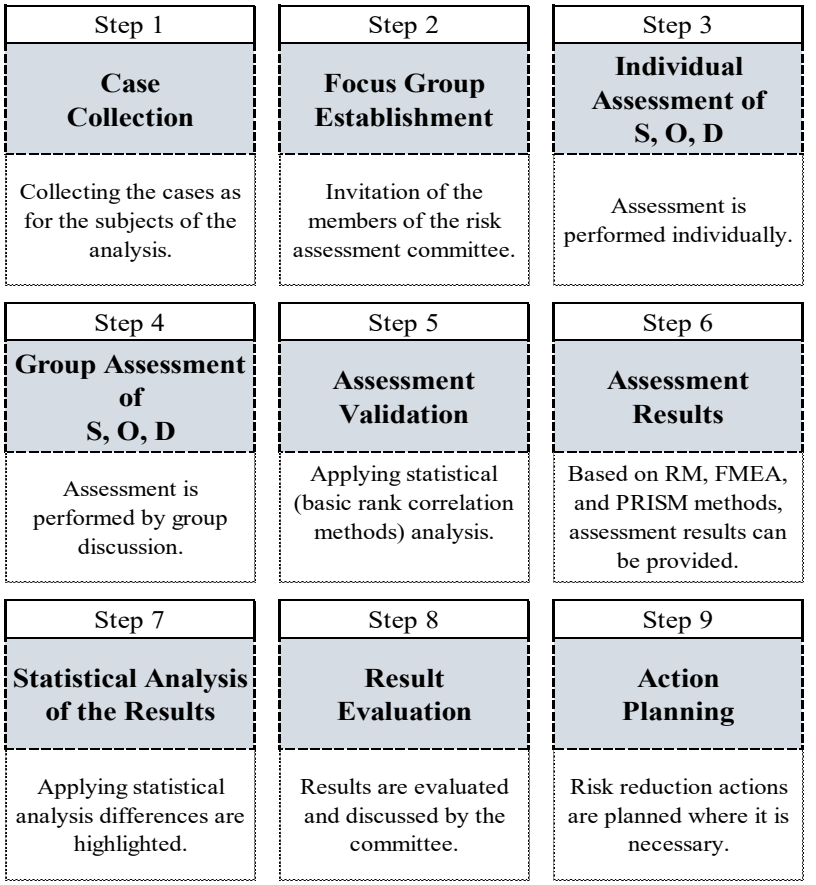

Figure 2
The designed risk assessment process

Table 1
The summary of individual and group assessments

	Individual assessments									Group assessments					
	Expert 1			Expert 2			Expert 3			Discussion-based			Aggregation of individual results		
Case	S	O	D	S	O	D	S	O	D	S	O	D	S	O	D
A	3	2	4	3	3	4	3	3	4	3	2	4	3	2,67	4
B	1	4	2	2	4	2	1	4	3	1	4	3	1,33	4	2,33
C	3	3	4	3	4	3	2	3	4	2	2	4	2,67	3,33	3,67
D	3	1	4	3	2	4	3	1	3	2	1	4	3	1,33	3,67
E	1	2	1	1	3	2	1	2	2	1	3	2	1	2,33	1,67
F	2	3	1	1	3	2	1	3	2	2	4	4	1,33	3	1,67

Table 1 includes the individual assessments, the discussion-based assessments, and the assessments based on aggregating the individual results.

As for step 5, the validation of the assessment results was executed. Since the subjective judgment rules of the experts can be significantly independent of the proposed ranking tables in [27], the assessment results had to be validated first. The offered validation process was described [27] based on an expert-by-expert comparison technique, and in the study, it was observed that the experts' rankings have no significant differences:

- the individual assessments of the experts could be aggregated (See the last three columns in Table 1);
- and the applied scales for assessing *S*, *O*, and *D* were interpreted as valid assessment scales.

Figure 3 shows the boundaries of the preceding studies and this article. The results related to the discussion-based PRISM method are described in detail in [19], while the aggregation-based FMEA results can be found in detail in [27].

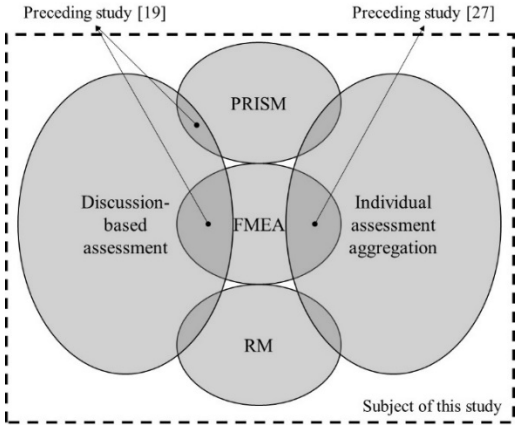

Figure 3
Boundaries of the preceding studies and this study

In step 6, the multi-criteria risk assessment of the compliance cases is performed by three risk assessment methods (RM, FMEA, PRISM) described in Section 2.1. Figure 4 shows the Risk Exposure-based, Figure 5 shows the RPN-based, while Figure 6 shows the PRISM-based assessments.

Different colors represent different Risk Exposure values, and based on Eq (1), the possible iso-risk lines in the Risk Matrix are linear (see Figure 4). The greener the matrix cell, the lower the Risk Exposure value, while the redder the matrix cell, the higher the Risk Exposure value. The iso-risk lines give the ranking of the assessments.

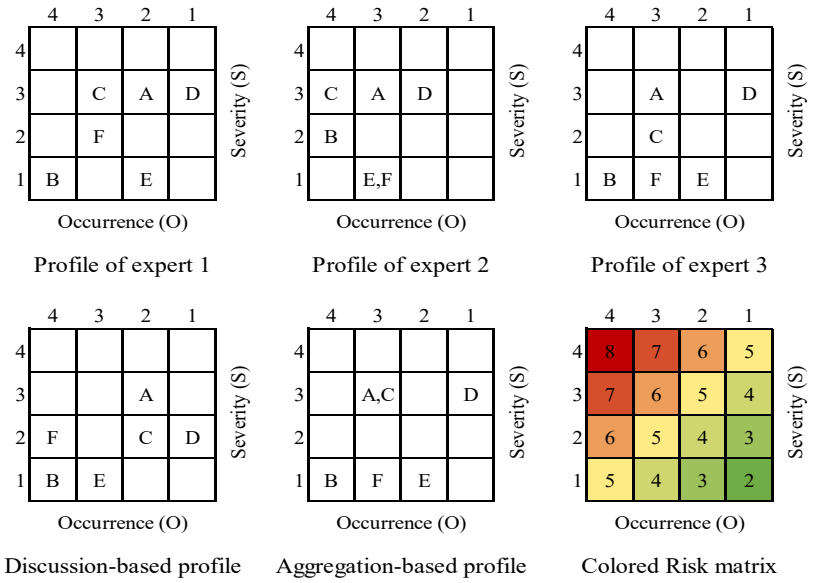

Figure 4
Risk Matrices with the assessed cases

The RPN values of the cases are visible in Figure 5. The greener the matrix cell, the lower the risk level, while the redder the matrix cell, the higher the risk level.

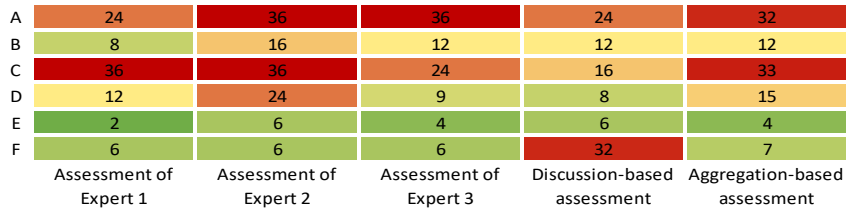

Figure 5
The Risk Priority Number of the cases

The PRISM-based assessments are visible in Figure 6. Based on Eq (3), the possible iso-risk lines in the Partial Risk Map are linear. A case is consistently ranked by its highest PRISM number.

Table 2 shows the dense ranks of the cases by methods and experts, while Table 3 shows the dense ranks by methods and group assessments. Based on descending order, the higher the case rank, the higher the risk.

Based on Table 2 and Table 3, the paper's assumptions are examined, and the results of the analyses are presented and interpreted in Section 3.

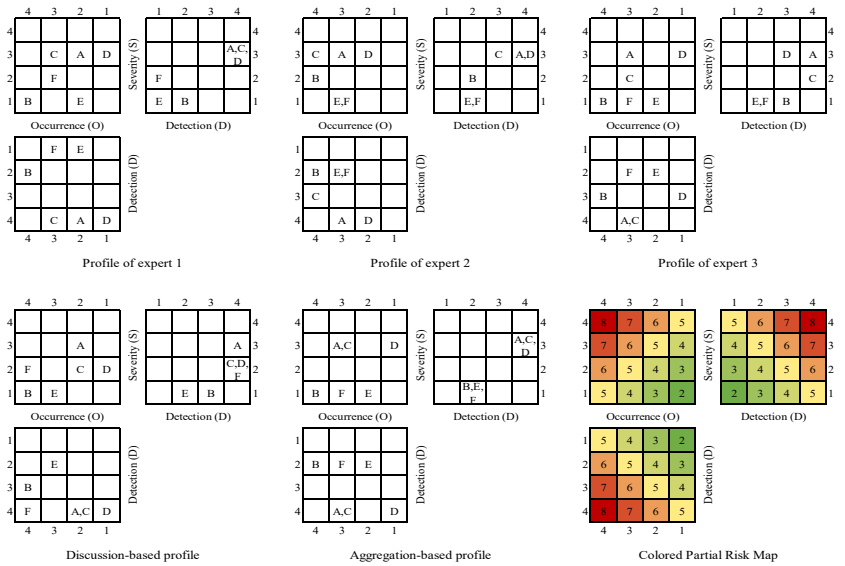

Figure 6
PRISM profiles with the assessed cases

Table 2
Individual ranking of the cases

	Risk Exposure			Risk Priority Number			PRISM number		
Case	Expert 1	Expert 2	Expert 3	Expert 1	Expert 2	Expert 3	Expert 1	Expert 2	Expert 3
A	2	2	1	2	1	1	1	1	1
B	2	2	2	4	3	3	2	2	1
C	1	1	2	1	1	2	1	1	1
D	3	3	3	3	2	4	1	1	2
E	4	4	4	6	4	6	4	3	4
F	2	4	3	5	4	5	3	3	3

Table 3
Discussion-based group assessment and aggregated ranking of the cases

	Discussion-based ranks			Aggregation-based ranks		
Case	Risk Exposure	Risk Priority Number	PRISM number	Risk Exposure	Risk Priority Number	PRISM number
A	2	2	2	1	2	1
B	2	4	2	2	4	2
C	3	3	3	1	1	1
D	4	5	3	3	3	1
E	3	6	4	4	6	4
F	1	1	1	3	5	3

3 Results

The first assumption's (A1) results are presented first. As step 7 of the risk assessment process, Table 4, Table 5, and Table 6 show the results of rank correlation analysis related to the three individual assessments and the two types of group assessments. Table 4 is related to the RM, Table 5 is related to the FMEA, and Table 6 is related to the PRISM method. The value of the Spearman's rho rank correlation coefficient is in the first matrix cell ("Sp. rho"), followed by the 2-tailed significance level ("Sig.").

Table 4
Correlations related to the RM-based comparisons

Group assessment	Individual assessment					
	Expert 1's rank		Expert 2's rank		Expert 3's rank	
	Sp. rho	Sig.	Sp. rho	Sig.	Sp. rho	Sig.
Discussion-based rank	0,375	0,464	-0,136	0,797	0,303	0,559
Aggregation-based rank	0,844	0,035	0,909	0,012	0,955	0,003

There are no significant correlations between individual ranks of the experts and discussion-based rank. On the other hand, between individual ranks of the experts and aggregation-based rank, there are only significant results with high-rank correlation coefficient values.

Table 5
Correlations related to the FMEA-based comparisons

Group assessment	Individual assessment					
	Expert 1's rank		Expert 2's rank		Expert 3's rank	
	Sp. rho	Sig.	Sp. rho	Sig.	Sp. rho	Sig.
Discussion-based rank	0,314	0,544	0,206	0,695	0,429	0,397
Aggregation-based rank	1,000	0,000	0,971	0,001	0,886	0,019

There are no significant correlations between individual ranks of the experts and discussion-based rank. Between individual ranks of the experts and aggregation-based rank, there are only significant results with high-rank correlation coefficient values.

Table 6
Correlations related to the PRISM-based comparisons

Group assessment	Individual assessment					
	Expert 1's rank		Expert 2's rank		Expert 3's rank	
	Sp. rho	Sig.	Sp. rho	Sig.	Sp. Rho	Sig.
Discussion-based rank	0,031	0,953	-0,127	0,810	0,281	0,589
Aggregation-based rank	1,000	0,000	0,984	0,000	0,742	0,091

There are no significant correlations between individual ranks of the experts and discussion-based rank. However, except for the case of Expert 3, the results are significant with high-rank correlation coefficient values between individual ranks of the experts and aggregation-based rank.

Secondly, the second assumption's (A2) results are presented. Kendall's rank concordance analysis is performed based on the expert rankings. The results of the analysis are summarized in Table 7.

Table 7
Kendall's rank concordance analysis results

	RM	FMEA	PRISM
Kendall's W	0,842	0,948	0,877
Significance level	0,027	0,014	0,022

Based on the results, the FMEA-based aggregation of the individual results has the highest Kendall's W value. However, in the case of all methods, the consensus level is significantly high.

4 Discussion and Managerial Implications

4.1 Discussion

According to ISO 37301:2021 [14], the systematic compliance risk assessment process significantly impacts business sustainability. Enterprise risks and risk management are critical factors in the 21st Century's complex business environment [29]. Based on [14, 29], the introduced compliance risk assessment process aims for a systematic and multi-methodological assessment of compliance risks. Analyzing the complex compliance risks requires a rigorous assessment process, including various indicators [17].

According to the case study at three banks operating in Central Eastern Europe, the qualitative approach for the research process is necessary [30]. Following the PDCA (Plan, Do, Check, Act) cycle, the evaluation phase of improvement projects is essential. Intense compliance supervision is fundamental in ensuring a sound banking system [31, 32]. Thus, in this follow-up case study, analyses are built on reliable data [27], and the assessment is simultaneously based on three different methods. However, the cost of regulatory compliance in the banking sector increases significantly [33]. The proposed multi-model risk assessment method produces sound results without sensibly increasing the evaluation cost because the assessment methods build on the same input.

Since the failure of bank boards and top experts in risk assessment can result in ineffective risk management [34], the proposed assessment process focuses specifically on the internal operations of the assessment board. Based on the proposed process, the results highlight some critical operation features that are useful to be discussed. The case study results highlight the importance of individual assessments, even in expert teams.

Since the ranking of the compliance risks is a multi-criteria decision-making process, the individual assessments can be helpful in the characterization and validation of the decision-making process. Individual risk assessment of complex phenomena leads to different rankings [27, 35]. Thus, differences between group assessments and individual assessments can be interpreted. Based on the results of this case study, there is a chance to have very different rankings if the assessment process is based on group discussion or individual assessment aggregation. Following the offered assessment process steps of this study can highlight the nature of the differences.

Significant differences were observed between discussion-based and aggregated rankings in this case study. The correlation between individual and aggregated rankings is higher than between individual and discussion-based rankings (see Assumption 1). The applied risk assessment methodology has no significant impact on the results of the assessments. Reflecting the necessity of sound bank systems [32] and effective risk management [34], focusing on the individual assessment level is essential. However, differences between rankings can be lower or higher in other banks, compliance fields, or other compliance cases. This study and its predecessor study [27] highlight the usefulness of individual assessments' operational analysis in the compliance assessment process.

Based on the results related to the consensus level of the individual assessments, no significant difference can be observed between the applied methods. The highest consensus level is observed in the case of FMEA, so the individual assessments were the most closely in the case of rankings by RPN (See Assumption 2). Instead of cases where only one method is applied [17], the research suggests applying more than one risk assessment method in the case of complex phenomena assessment. Thus, testing the validity of the individual assessment process step can be executed, and the inputs for the result evaluation will be more reliable.

A limitation of the study is that a limited number of experts considered the compliance cases. As for disseminating the multi-method risk assessment process, these numbers are enough, but the research can be performed again with an increased number of experts in the future. Furthermore, since risk factors are estimated based on previous observations, some uncertainty is associated with these estimations. Considering this uncertainty is a possible direction of extension to the proposed assessment process, like the measurement uncertainty consideration in forecasts and risk-based decisions [36, 37].

This study stops at the statistical analysis of the results (step 7). First, according to the change management process model in [38], it is essential to evaluate the assessment results, as shown in Step 8 and Step 9 in Figure 2. Step 8 refers to the discussion of the results by the expert group or committee, which should include identifying lessons learned in the evaluation process. Additionally, some knowledge or skill gaps may be defined at this point. Next, step 9 is about planning risk reduction action. Following the PRISM and FMEA methods, risk reduction can aim at either decreasing the severity of consequences (i.e., insurance or technology improvements), decreasing the probability of occurrence (i.e., with statistical control activities), or increasing the detectability of the failure, by new controls or alarm points or training. In the banking sector, following the traditional audit risk model, measures may aim at the incentive system or internal control system, like board structure or reporting. Finally, the risk of attitude or rationalization may be affected by training and education. [39, 40]

4.2 Managerial Implications

The senior management is responsible for determining the company's compliance policy, including the commitment to produce and sell only compliant products and to comply with applicable regulations and industry standards. In addition, top management seeks tangible evidence of returns on efforts to continue compliance improvement programs. Thus, based on the research results, operations research can help transform compliance management into a more reliable process.

A risk-based approach is the general best practice for compliance management, as described in Section 1. The three risk assessment techniques described in Section 2 contribute to a better understanding of techniques and a choice among them for better decision-making. The authors suggest supplementing the risk analysis of ISO 37301:2021 with the "undetection" dimension, as used in FMEA and PRISM methods [19].

The individual assessment of risks should be supplemented to the group-level assessment in the risk assessment process. At the end of the assessment process, more detailed risk mitigation actions can be planned. From a management perspective, following the designed compliance risk assessment process (See Figure 2) helps leaders and responsible risk owners to address compliance risks. The proposed process can be used as a comprehensive tool to select the necessary compliance measures optimally. The authors consider compliance a strong business driver, in line with quality and reliability management, that can lead to business sustainability [41].

Conclusions

This study provides insight into compliance risk assessment methodologies. Previous studies have focused on the discussion-based PRISM method [19] and the aggregation-based FMEA [27]. This follow-up case study complements the above

with statistical analysis to investigate the consensus level of the participants while the assessment is simultaneously based on three different methods.

First, a brief introduction to compliance management describes the organizational function responsible for fulfilling legal, regulatory, industrial, and other obligations. Then, Section 1 describes the three distinguished steps of the compliance risk assessment process.

The steps of the empirical research and the materials used are presented in Section 2. The primary data collection was at one of the largest commercial banks in Central and Eastern Europe in 2021. In a previous study [27], the authors applied the FMEA in compliance risk assessment in the financial sector for the first time. The results are shown in Section 3. The authors validated the interpretations from the case study through consensus analysis. In this paper, two assumptions have been examined.

Regarding the first assumption, the results highlight no significant correlations between individual rankings of the experts and discussion-based ranking. However, the results are significant and have high-rank correlation coefficient values between individual and aggregation-based rankings (except for the case of Expert 3 in the PRISM-based comparisons). This study highlights the usefulness of individual assessments of experts in the compliance risk assessment process.

As for the second assumption, the results show that the FMEA-based aggregation of the individual results has the highest consensus level. However, in the case of all methods, the consensus level is significantly high. Therefore, this research suggests applying more than one risk assessment method in the case of complex phenomena assessment, just like bank compliance issues. Thus, testing the validity of the individual assessment process step can be executed, and the inputs for the risk evaluation will be more reliable.

The results are discussed in Section 4. The results related to the discussion-based PRISM method are described in detail in [19], while the aggregation-based FMEA results can be found in detail in [27]. One key finding of this study is that individual assessments can help characterize and validate the decision-making process. No significant difference can be observed between the applied methods, while testing the validity of each step of the evaluation process is possible.

Future research will focus on further developments of the PRISM method. One possible developmental direction is to combine the PRISM methodology with MCDM methods to understand better the complexity of the risk assessment characteristics of the banking sector. The research related to PRISM integration with pairwise comparison and other MCDM techniques has already started as a possible methodological development direction. Currently, the first integration experiences related to AHP (Analytic Hierarchy Process), BWM (Best Worst Method), and TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) are being synthesized. Furthermore, since applying fuzzy sets provides excellent possibilities in the bank risk description under uncertainty [42-44], fuzzification is the upcoming developmental direction of the PRISM method.

The authors also plan to repeat the research with an increased number of experts and incidents to characterize more deeply the possible differences in the applied methods. Furthermore, future research will examine how the proposed compliance assessment process can be integrated with business risk assessments based on the PRISM approach. Finally, investigating the relationship between organizational resilience and compliance management is a topic with great potential.

References

[1] Ramos-González, M. D. M.; Rubio-Andrés, M.; Sastre-Castillo, M. Á.: Building Corporate Reputation through Sustainable Entrepreneurship: The Mediating Effect of Ethical Behavior, Sustainability 2017, 9, 1663, https://doi.org/10.3390/su9091663

[2] Eizenberg, E.; Jabareen, Y.: Social Sustainability: A New Conceptual Framework, Sustainability 2017, 9, 68, https://doi.org/10.3390/su9010068

[3] Wells P.: Sustainable business models and the automotive industry: A commentary, Centre for Automotive Industry Research, Cardiff Business School, Cardiff, UK, 2013

[4] Yamane, T.; Kaneko, S.: The sustainable development goals as new business norms: A survey experiment on stakeholder preferences, Ecological Economics 2022, 107236, https://doi.org/10.1016/j.ecolecon.2021.107236

[5] Surman, V.; Böcskei, E.: Examining Sustainability Attitudes in the case of Small and Medium-sized Enterprises, In Proceedings of FEB Zagreb 2022, 13th International Odyssey Conference on Economics and Business, Dubrovnik, Croatia, 1-4 June, 2022

[6] EU Regulation 2020/852. Available online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32020R0852&from=EN (accessed on 30 April 2022)

[7] EU Regulation 2021/2178. Available online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32021R2178&from=EN (accessed on 30 April 2022)

[8] Wong, C. M. L.; Jensen, O.: The paradox of trust: perceived risk and public compliance during the COVID-19 pandemic in Singapore, Journal of Risk Research 2020, 23, pp. 1021-1030, https://doi.org/10.1080/13669877. 2020.1756386

[9] Stupak, I., Mansoor, M.; Smith, C. T.: Conceptual framework for increasing legitimacy and trust of sustainability governance, Energy, Sustainability and Society 2021, 11, https://doi.org/10.1186/s13705-021-00280-x

[10] Harkácsi, G. J.; Szegfű, L. P.: The Role of the Compliance Function in the Financial Sector in the Age of Digitalisation, Artificial Intelligence and Robotisation, Financial and Economic Review 2021, 20, pp. 152-170

[11] Poppensieker, T.; Schneider, S.; Thun, M.: Financial institutions and non-financial risk: Learning from the corporate approach, in: Non-Financial Risk Management: Emerging stronger after Covid-19, 1st Ed.; Kaiser, T., Risk Books: London, United Kingdom, 2021

[12] Hendra, R.: Comparative Review of the Latest Concept in Compliance Management & The Compliance Management Maturity Models, RSF Conference Series: Business, Management and Social Sciences 2021, 1, 116-124, https://doi.org/10.31098/bmss.v1i5.457

[13] Holter Antonsen, H.; Madsen, D. Ø.: Developing a Maturity Model for the Compliance Function of Investment Firms: A Preliminary Case Study from Norway, Adm. Sci. 2021, 11, 109. https://doi.org/10.3390/admsci11040109

[14] ISO: Compliance management systems - Requirements with guidance for use. ISO 37301:2021

[15] IEC: Risk management — Risk assessment techniques 31010:2019, 2019

[16] Basel Committee on Banking Supervision: Principles for Effective Risk Data Aggeration and Risk Reporting, 2013, http://www.bis.org/publ/bcbs222.pdf 22/08/2021

[17] Losiewicz-Dniestrzanska, E.: Monitoring of compliance risk in the bank, Procedia Economics and Finance 2015, 26: 800-805, https://doi.org/10.1016/S2212-5671(15)00846-134

[18] Mirghafori, S. H.; Takalo, S. K.; Dastranj, M.: Banking service quality management using fuzzy FMEA (a case study: Central Melli Bank of Rafsanjan), International Journal of Quality and Innovation 2016, 3, 1-16, https://doi.org/10.1504/IJQI.2016.079907

[19] Bognár, F.; Benedek, P.: A Novel Risk Assessment Methodology – A Case Study of the PRISM Methodology in a Compliance Management Sensitive Sector, Acta Polytechnica Hungarica 2021, 18, 89-108, https://doi.org/10.12700/APH.18.7.2021.7.5

[20] Qazi, A., Shamayleh, A., El-Sayegh, S., Formaneck, S.: Prioritizing risks in sustainable construction projects using a risk matrix-based Monte Carlo Simulation approach, Sustainable Cities and Society, 65, (2021) 102576, https://doi.org/10.1016/j.scs.2020.102576

[21] Wang, R.; Wang, J.: Risk Analysis of Out-drum Mixing Cement Solidification by HAZOP and Risk Matrix, Annals of Nuclear Energy, 2020, 147, 107679, https://doi.org/10.1016/j.anucene.2020.107679

[22] Liu, H. C.; Liu, L.; Liu, N.: Risk evaluation approaches in failure mode and effects analysis: A literature review, Expert Systems with Applications 2013, 40, 828-838, https://doi.org/10.1016/j.eswa.2012.08.010

[23] Bognár, F.; Hegedűs, Cs.: Description and Consequences on some Aggregation functions of PRISM (Partial Risk Map) Risk Assessment Method, Mathematics, 2022, 10, 676, https://doi.org/10.3390/math10050676

[24] Braglia, M. MAFMA: Multi-attribute failure mode analysis, International Journal of Quality and Reliability Management 2000, 17, 1017-1033, https://doi.org/10.1108/02656710010353885

[25] Spearman, C.: The Proof and Measurement of Association between Two Things, The American Journal of Psychology, 1904, 15, 72-101, https://doi.org/10.2307/1412159

[26] Kendall, M. G.: Rank Correlation Methods, Griffin: London, UK, 1970

[27] Bognár, F.; Benedek, P.: Case Study on a Potential Application of Failure Mode and Effects Analysis in Assessing Compliance Risks, Risks 2021, 9, 164, https://doi.org/10.3390/risks9090164

[28] Berényi, L.; Deutsch, N.: Corporate Social Responsibility and Business Philosophies among Hungarian Business Students, Sustainability 2021, 13, 9914, https://doi.org/10.3390/su13179914

[29] Strelicz, A.: Risks and threats in cyberspace – The key to success in digitalization, Journal of Physics Conference Series 2021, 1935, 012009, https://doi.org/10.1088/1742-6596/1935/1/012009

[30] Bauer, S.; Bernroider, E. W. N.; Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks, Computers & Security 2017, 68, 145-159, https://doi.org/10.1016/j.cose.2017.04.009

[31] Demirgüç-Kunt, A.; Detragiache, A.; Tressel, T.: Banking on the principles: Compliance with Basel Core Principles and bank soundness, Journal of Financial Intermediation 2008, 17, 511-542, https://doi.org/10.1016/j.jfi.2007.10.003

[32] Demirgüç-Kunt, A.; Detragiache, A.: Basel Core Principles and bank soundness: Does compliance matter?, Journal of Financial Stability 2011, 7, 179-190, https://doi.org/10.1016/j.jfs.2010.03.003

[33] Kaminski, P.; Mikkelsen, D.; Poppensieker, T.; Robu, K.: Sustainable compliance: Seven steps toward effectiveness and efficiency, McKinsey & Company 2017, 1-9

[34] Agarwal, S.; Kamath, S.; Subramanian, K., Tantri, P.: Board conduct in banks, Journal of Banking & Finance, 2022, 106441, https://doi.org/10.1016/j.jbankfin.2022.106441

[35] Qin, J.; Xu, Y.; Pedrycz, W.: Failure mode and effects analysis (FMEA) for risk assessment based on interval type-2 fuzzy evidential reasoning method, Applied Soft Computing, 2020, 89, 106134, https://doi.org/10.1016/j.asoc.2020.106134

[36] Hegedűs, Cs.; Kosztyán Zs. T.: The consideration of measurement uncertainty in forecast and maintenance related decisions, Problems of Management in the 21st Century 2011, 1, pp. 46-69, https://doi.org/10.33225/pmc/11.01.46

[37] Kosztyán, Zs. T.; Hegedűs, Cs.: Computer-Aided Diagnostic Methods to Forecast Condition-Based Maintenance Tasks, Lecture Notes in Electrical Engineering 2013, 151, 367-380, https://doi.org/10.1007%2F978-1-4614-3558-7_30

[38] Horváth, Cs.; Mecsei, I.: Sustainability Inspections in Printing Industry, International Joint Conference on Environmental and Light Industry Technologies. 19-20 November 2015 Budapest, Hungary Obuda University pp. 19-24

[39] Cressey, D. R.: Other People's Money, 1973, Patterson Smith, Montclair

[40] Fortvingler, J.; Szívós, L.: Different Approaches to Fraud Risk Assessment and Their Implications on Audit Planning, Periodica Polytechnica Social and Management Sciences, 2016, 24(2), pp. 102-112, https://doi.org/10.3311/PPso.8436

[41] Aigner, D. J.; Hopkins, J.; Johansson, R.: Beyond Compliance: Sustainable Business Practices and the Bottom Line, American Journal of Agricultural Economics 2003, 85, pp. 1126-1139, https://www.jstor.org/stable/1244884

[42] Cao, C.; Zhang M.: Credit Risk Evaluation of Quantum Communications Listed Companies in China Based on Fermatean Fuzzy TOPSIS, Procedia Computer Science, 2022, 199, pp. 361-368, https://doi.org/10.1016/j.procs.2022.01.044

[43] Yuanyuan Zhou, Y.; Zheng, c.; Goh, M.: Statistics-based approach for large-scale group decision-making under incomplete Pythagorean fuzzy information with risk attitude, Knowledge-Based Systems, 2022, 235, 107654, https://doi.org/10.1016/j.knosys.2021.107654

[44] Bonet, I.; Peña, A.; Lochmuller, C.; Patiño, H. A.; Chiclana, F.; Góngora, M.: Applying fuzzy scenarios for the measurement of operational risk, Applied Soft Computing, 2021, 112, 107785, https://doi.org/10.1016/j.asoc.2021.107785