A Novel Risk Assessment Methodology – A Case Study of the PRISM Methodology in a Compliance Management Sensitive Sector

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: The paper introduces the PRISM methodology built on the critical characteristics of the traditional failure mode and effect analysis (FMEA) and the risk matrix (RM) risk assessment methodologies. The authors create a new definition in the risk assessment process, which is introduced as partial risk. The paper focuses on assessing the compliance risks, the risks of organizational wrongdoing, and legal non-compliance. A real-life case study from the banking sector shows the risk assessment process based on the PRISM method.

Keywords: risk assessment; FMEA; risk matrix; compliance management

Introduction

The current global pandemic and economic crisis have directed the public and legislative focus on risk management and risk prevention. How an organization manages uncertainty can have crucial effects on the customer experience, reputation, competitiveness, and sustainability. Compliance management is a few decades-old business approach to keeping up with fast-changing legal and business requirements. [1] By definition, the purpose of internal controls is to ensure compliance with laws and regulations, the efficiency and effectiveness of the operations, and the credibility of the financial reports. Over the last 20 years, new regulations are being created to such an extent and quantity that compliance with them has become an independent task. This phenomenon has given rise to the organizational function of compliance management. The core definition of compliance is obeying various pieces of internal and external legislation. More recently, a more comprehensive perspective incorporates following the letter and the spirit of the legislation. *Compliance management* is a support function that aims to manage or minimize the risks of organizational wrongdoing and legal non-

compliance. Like data loss or information privacy, IT compliance issues affect every department of any organization's daily procedures.

This paper focuses on the presentation of a novel risk assessment methodology via the evaluation of compliance risks. We assume that a combined Failure Mode and Effects Analysis (FMEA) and Risk Map (RM) method can be applied to assess and monitor different kinds of risks, like compliance-related risks. Using the previously mentioned method, organizations would formulate measures for the organization's current, individual operation to reduce error modes' frequency or improve failure and error detection.

This research examines how suitable are the new combined FMEA and RM method in the risk assessment and evaluation of financial service companies' compliance organizations.

The first part of the article is an overview of compliance management, focusing on compliance risk assessment. The essence of the compliance concept is a social and economic interpretation, a novelty that assesses non-compliance as a risk. This risk consists primarily of two factors: regulatory risk and reputational risk. In this part, we introduce the relevant standards like ISO 31000: 2018, IEC 31010: 2019, ISO / IEC 27005: 2018, and ISO 19600: 2014 guidelines.

In the second part, the traditional concept of FMEA and Risk Map is presented. The first method aims to identify the existing or possible failures and their cause, estimating the failures' risks. Risk matrices apply two rating factors, which are used to estimate the "probability" and the "impact" dimensions.

In the following part, we present the concept of partial risk and the new PRISM method based on a unique combination of FMEA and risk maps. Later, a case study from the banking sector shows the practical implementation of the newly proposed method. A discussion and further research hypothesis close this paper.

1 Risk Evaluation in Compliance Management

The first significant compliance management publications describe the relations among transparency, business ethics, and compliance. [2, 3] The post-millennium scandals brought the relevant thematic boom. Standing out of the many was the Turner Review [4], which analyzed the management theory of the global banking crisis, Silverman's comprehensive organizational Compliance Management [5] and the Governance, Risk and Compliance Handbook [6].

The US is serving with the most prominent examples of expectations of corporate compliance systems. The Federal Sentencing Guidelines for Organizations last amended in 2018 [7, 8], the Sarbanes-Oxley Act from 2002 [9, 10], and the COSO Internal Control–Integrated Framework [11, 12] stand as guidelines for the

minimum requirement for today's compliance systems. Each organization can tailor its use of the above to its business, and other standards related to the professional profile may also be relevant.

Major international organizations (e.g. UN, World Bank), as well as national governments, have also developed and published several general and thematic directives and best practice recommendations, such as the updated OECD Principles on Corporate Governance (2015), the Corporate Responsibility to Respect Human Rights (2003), UN Global Compact (2000), UN Principles for Responsible Investment (2006).

All business activities are risky to some extent, and these risks can be measured, analyzed, reduced, managed, i.e. kept below a certain level. The task of risk management is to keep the probability of possible effects occurring at some conscious level. Compliance mainly focuses on legal and regulatory requirements. According to a strict approach, legality is not a matter of consideration but merely a requirement. According to the standard approach, compliance manages unique compliance risks. In many cases, the interpretation of legislation gives decision-makers a degree of freedom so that discretion does not appear at the level of taking or rejecting a particular risk but at how 'compliant' is any given solution [13].

Compliance risk consists primarily of two factors: penalties for non-compliance and reputational risk. *Regulatory risks* are assessed based on the potential penalty and the likelihood of falling. There is a relatively straightforward risk level above which compliance officers vetoe the risky decision or product in question. On the one hand, the regulations, requirements, and legislation changes that apply to the organization must be monitored. The tasks, risks, and responsibilities associated with the given legislation or change must be defined.

On the other hand, all other compliance activities provide information on where the organization is facing deficiencies or errors concerning its objectives and how risk management can be continuously improved. The goal of compliance is not to build a bottom-up system of legal references but vice versa. Based on international practices and experiences, each organization defines the relevant compliance risks. Compliance fundamentally incorporates developing a risk management methodology and planning and implementing internal controls related to the specific compliance risks.

Reputational risk is different in different markets. On the one hand, it is a reputational risk that customers become unloyal due to an incident. More importantly, if the organization becomes risky, it can lose its partners, which is a severe threat to its operations. For example, in the spring of 2018, the Latvian bank ABLV was liquidated weeks after it was suspected of connecting to North Korea's weapons development program [14]. All market participants reacted to the news by closing the partnership. If the information, data, customer due diligence, or anything is unreliable and laundered money comes in, that is unacceptable.

Reputational risk is a powerful motivation to operate a robust compliance function.

There is a worldwide effort to define a quality assurance framework for compliance by standards. We would like to highlight ISO 31000: 2018, IEC 31010: 2019, ISO / IEC 27005: 2018, and ISO 19600: 2014 guidelines.

ISO 31000: 2018 guides how to manage the risks faced by organizations. Every organization tailors these guidelines to its environment and operation in practice. The guidelines help in any activity, including decision-making, at all levels. Based on the guidelines' foreword, we would like to focus on two main changes from the 2009 version.

1) "highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;
2) greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge, and analysis can lead to a revision of process elements, actions, and controls at each stage of the process. " [15]

The importance of iterative risk management returns in several places in the text; the idea of continuous improvement of Total Quality Management (TQM). The emphasis on leadership and commitment, as well as inclusive responsibility ("Everyone in an organization has responsibility for managing risks." [16]), is also in line with the TQM philosophy.

IEC 31010: 2019 guides the selection and application of risk assessment techniques that help make decisions when there is uncertainty [17]. The 2019 edition of the guidelines contains summaries of an increased number of techniques, referring to other documents which describe the methods and techniques in more detail. "The standard is useful both as part of a process to manage risk and when comparing options and opportunities so that decisions are based on a good understanding of risk," said Professor Jean Cross [18].

ISO 27005: 2018 is designed to help implement information security based on a risk management approach [19]. This standard applies to any organization that seeks to address risks that could compromise its information security.

ISO 19600: 2014 Compliance Management Systems is currently one of the most critical international recommendations for business compliance management, which describes the cooperation between compliance assurance and risk management [20]. The "AS 3806 - Compliance Programs" standard established in the Australian financial sector in 1998, updated in 2006, is the document's predecessor. The document's cited sources show that this directive relates to ISO 9001, the ISO 10002 complaint handling standard, and the social responsibility guidelines (ISO 26000). The 19600: 2014 guidelines for compliance management

systems are close to the ISO 31000 risk management standard. Table 1 shows the comparison of the processes in two documents.

Table 1
Management processes in ISO standards, not exhaustive

ISO 31000: 2018	ISO 19600: 2014
Communication and consultation	Communication
Creating the context (Scope, context, criteria)	Creating the context (Scope, context, criteria) and Developing a Compliance Management System
Risk identification	Identification of compliance obligations and related compliance risks
Risk analysis	Risk analysis - the probability and impact of non-compliance
Risk evaluation	Risk evaluation - prioritization
Risk treatment	Risk treatment - planning and implementation of controls
Recording and Reporting	Performance Evaluation and Compliance Reporting

Source: own editing based on ISO 31000: 2018 and ISO 19600: 2014

Every organization is unique. Therefore, compliance systems differ depending on the industry and specific risks. At the same time, good practices outlined in ISO 19600:2014 cover specific areas of ethical corporate operation and serve as guidelines for organizations. According to ISO 19600:2014, integrity and compliance could be considered an opportunity for developing a successful and sustainable organization.

The ISO 19600:2014 standard facilitates the design, implementation, evaluation and maintenance of the compliance system. In the flowchart (Figure 1), the modified PDCA cycle's first step is to identify compliance obligations and evaluate compliance risks. The second step is to address these risks and set measurable objectives related to them. Planning is followed by operation and control of the compliance risks. Per the logic of the PDCA cycle, implementation is followed by performance evaluation and reporting. The outcome of performance evaluation is getting a systematic overview of the strengths and the weaknesses of the system, highlighting the areas for possible development. The fourth step is the management of non-compliance and the continual improvement of the system. Similar to ISO 9001:2015, leadership is a critical factor that ensures all the other flowchart elements cooperate properly.

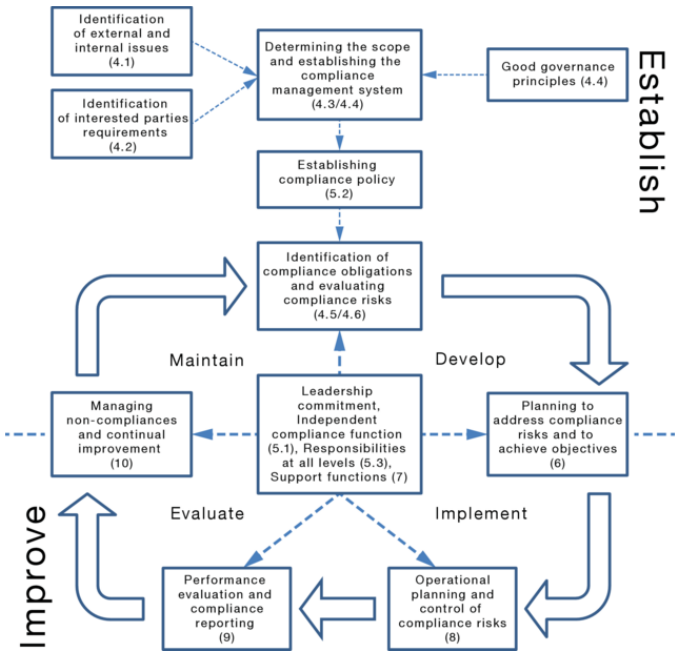

Figure 1
Flowchart of a compliance management system

Source: ISO 19600: 2014 [21]

Compliance management is aligned with risk management in the general sense. The standard recognizes the risk-based approach to compliance. It is also familiar with the concept of complex risk appetite, the extent to which an investor or organization is willing to take risks. In the following chapters of this paper, a new methodology is presented to provide a practical approach to compliance risk evaluation.

2 Risk Assessment Based on the Failure Mode and Effect Analysis (FMEA) and the Risk Matrix (RM)

Failure mode and effect analysis (FMEA) is a widely applied and developed methodology. The methodology is performed continuously in most manufacturing industries and developed by researchers in numerous research papers. [22] Nowadays, the most dominant research development field of FMEA is based on multi-criteria decision making (MCDM) methodologies. [23]

2.1 Failure Mode and Effect Analysis

The FMEA methodology is applied to assess the risks of potential or existing failures in particular objects and prevent these failures from occurring. FMEA can significantly improve the reliability of different complex systems from technology-based services to all production fields. In the last years, many case studies were published related to the development of FMEA in connection with the IT sector. Case studies introduce the application of FMEA in highly IT-relevant fields, just like internet banking services [24] and healthcare systems. [25]

The traditional concept of FMEA is to identify the existing or possible failures and their cause, estimating the risks of the failures and reducing the risk of the failure. The target field of the analysis is traditionally a product or a process. First, a cross-functional team is set up to identify the relevant existing or possible failures using creative techniques. Identifying the failures can be a long process, depending on the nature, complexity, and size of the particular product or process. Once the cross-functional team identifies the failures, the team performs the risk analysis phase of the methodology.

The most crucial goal of the risk analysis is to determine the resultant value of each failure risk. This value is typically interpreted as a Risk Priority Number (RPN) and calculated using three rating factors. The value of occurrence (O), severity (S) and detection (D) is generally applied in the assessment process of the RPN. We calculate RPN as follows

$$RPN = OxSxD \tag{1}$$

where O is the probability of failure, S is the severity of the failure effect, and D is the probability of non-detecting the failure. The value of these rating factors can be estimated using numerous ways. For obtaining the RPN of a specific failure mode, the three risk factors are evaluated using different ten-point scales.

There has been a broad consensus in the research community on which scales should we evaluate each rating factor in recent decades. [26-30] However, in practice, the scales are often transformed to meet the analyzed product or process's measurement or estimation requirements. Based on the literature review of Liu [22], we apply Tables 2-4 to evaluate the three rating factors.

Table 2
Ratings for the occurrence [22]

Probability of failure	Possible failure rates	Rank
Extremely high: failure almost inevitable	≥ in 2	10
Very high	1 in 3	9
Repeated failures	1 in 8	8
High	1 in 20	7
Moderately high	1 in 80	6

Moderate	1 in 400	5
Relatively low	1 in 2000	4
Low	1 in 15000	3
Remote	1 in 150000	2
Nearly impossible	≤ 1 in 1500000	1

Table 3

Ratings for the severity [22]

Effect	Criteria: severity of the effect	Rank
Hazardous	Failure is hazardous and occurs without warning. It suspends the operation of the system or involves non-compliance with government regulations.	10
Serious	Failure involves hazardous outcomes or non-compliance with government regulations or standards.	9
Extreme	The product is inoperable with a loss of primary function. The system is inoperable.	8
Major	Product performance is severely affected but functions. The system may not operate.	7
Significant	Product performance is degraded. Comfort or convince functions may not operate.	6
Moderate	Moderate effect on product performance. The product requires repair.	5
Low	Small effect on product performance. The product does not require repair.	4
Minor	Minor effect on product or system performance.	3
Very minor	Very minor effect on product or system performance.	2
None	No effect.	1

Table 4

Ratings for the detection [22]

Detection	Criteria: the likelihood of detection by the design control	Rank
Absolute uncertainty	Design control does not detect a potential cause of failure or subsequent failure mode, or there is no design control.	10
Very remote	Very remote chance that the design control will detect a potential cause of failure or subsequent failure mode.	9
Remote	Remote chance that the design control will detect a potential cause of failure or subsequent failure mode.	8
Very low	Very low chance that the design control will detect a potential cause of failure or subsequent failure mode.	7
Low	Low chance that the design control will detect a potential cause of failure or subsequent failure mode.	6
Moderate	Moderate chance that the design control will detect a potential cause of failure or subsequent failure mode.	5
Moderately high	Moderately high chance that the design control will detect a potential cause of failure or subsequent failure mode.	4

High	High chance that the design control will detect a potential cause of failure or subsequent failure mode.	3
Very high	Very high chance that the design control will detect a potential cause of failure or subsequent failure mode.	2
Almost certain	Design control will almost certainly detect a potential cause of failure or subsequent failure mode.	1

The higher the factor-related risk of a particular failure mode, the higher the rating factor's value. The higher the overall risk of a particular failure mode, the higher the RPN value. Based on the RPN value, the failure modes can be prioritised to find the riskiest failure modes. If it is necessary, the prioritisation can be applied based on a specific rating factor as well. This step is essential since there are not enough resources to reduce all the possible risks in a product, machine or process. Thus, based on the prioritisation, the focus can be on the most important – so on the riskiest – failure modes. The riskiest failure modes are being placed under investigation for reducing the risk by proper actions. After the corrective actions, the rating factors' values are estimated again, so the iteration starts again.

2.2 Risk Matrix (RM)

Risk matrices represent another widely applicable group of risk assessment methodologies. Similar to the FMEA methodology, the risk matrix is built up by rating factors developed to assess a particular object's risk. [31] While FMEA applies three rating factors, risk matrices apply only two rating factors, which are usually used to estimate the "occurrence" and the "severity" dimensions. [32] Thus, the risk assessment tool's general structure is a matrix, as visible in Figure 2.

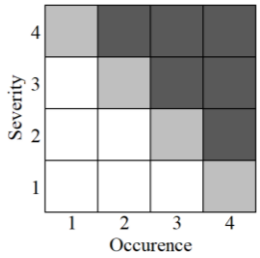

Figure 2
An example of the structure of the risk matrix

In general, the methodology estimates the risk on a 1-3 or 1-4 or 1-5 scale. Similarly to the FMEA, the higher the factor-related risk of a specific failure mode, the higher the rating factor's value. It often occurs that the rating factors of the risk matrix have different scale lengths. Thus, the risk matrix has a non-equal number of rows and columns.

The risk assessment is based on the score of the “occurrence” and “severity” assessment factors. If both the rating factors have high values, the associated risk

will be judged high, while when the rating factors have low values, they will be interpreted as low. As shown in Figure 2, the darker the colour of a matrix cell, the higher the associated risk of the failure mode.

As for the risk assessment result, different action categories are available for further steps, aiming to reduce the determined risk level. Based on the matrix cell's colour and the risk level, different actions can be launched, from the "no action needed" category to the "immediate intervention" action. Thus, the methodology classifies the failure modes into different groups, while the groups have ranks and failure modes have only group belonging identifications.

Both methodologies are powerful risk assessment tools that focus on developing the given product, process, or system. In the following part of the paper, we describe a methodology that builds on both the FMEA and the risk matrix's strengths, creating a new, more robust, and practical methodology.

3 The Definition of Partial Risk and the PRISM Methodology

There are failures in the business processes, systems, and products, which have strong connections with the compliance management system. These failures have relatively higher risk content than those processes, systems, and products, which are not directly compliance sensitive. In those sectors, where the compliance management systems have to be highly developed and linked to the organizational business processes, risk estimation has a more critical role than in other operational fields. In this chapter, a novel risk evaluation methodology is described, based on a combination of the failure mode and effect analysis and the risk matrix. Since both FMEA and RM have significant risk evaluation abilities, the new methodology is designed to build on the synergies of these abilities.

FMEA helps rank the risk of different failure modes and effects, and the methodology generally focuses on the value of the RPN. The problem is that multiplication can mask the detailed information held by each rating factor. A failure can have a low RPN value, while the failure's partial risk can be relatively high. Table 5 shows detailed examples of partial risk cases.

Table 5
Examples for partial risks

Case	Occurrence (O)	Severity (S)	Detection (D)	RPN
Case 1	1	10	5	50
Case 2	1	7	7	49
Case 3	10	4	1	40

As shown in Table 5, all the cases have a relatively low risk based on the RPN value. Nevertheless, a relatively small increase of the Occurrence rating factor value can significantly raise the RPN value at “Case 1” as well as at “Case 2”, while a slight increase of the “Detection” rating factor value of “Case 3" results in a significant increase in the RPN value. When the result of a multiplication of two rating factors is high, while the third rating factor's value is relatively low, the case of partial risk emerges.

A three-time risk matrix evaluation can amend the failure mode and effect analysis for the detailed risk estimation of failure modes. Risk matrices can evaluate the partial risks based on three different contexts: “occurrence vs. severity” and “occurrence vs. detection”, and “severity vs. detection”. All three analyses should be performed at the same time for gathering all the necessary information on the possibly existing partial risks. Figure 3 shows the map of the three different, partial analyses.

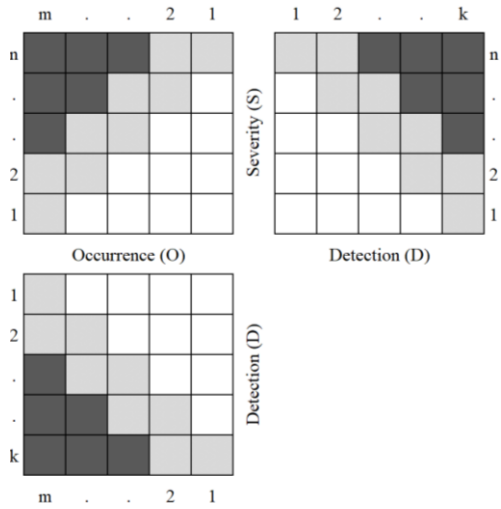

Figure 3

The general model of the PRISM (Partial Risk Map) risk evaluation methodology

In the general model, rating factors have the same scale length, so “k”, “n”, and “m” values are equal to each other. However, the scale length could be different if the practical case requires that. Furthermore, all the "k", "n" and "m" values can be different.

The colourings of the map are similar to the traditional risk matrix. Thus, the darker the colour of a matrix cell, the higher the failure mode's hidden risk. The map's colourings are changeable related to the practical problem and the application field.

According to the PRISM methodology, a failure mode could be determined as a potentially risky failure mode if any of the forthcoming criteria are fulfilled:

(1) the RPN value reaches a specific indicator value which the experts previously set;

(2) based on the values of the occurrence and severity rating factors, the failure mode position is inside that part of the O vs. S matrix, which was set to be risky;

(3) based on the values of the occurrence and detection rating factors, the failure mode position is inside that part of the O vs. D matrix, which was set to be risky;

(4) based on the values of the severity and detection rating factors, the failure mode position is inside that part of the S vs. D matrix, which was set to be risky.

If criterion (1) is fulfilled without fulfilling any other criteria, the failure mode could be considered risky because of the overall RPN value. If any of the criteria (2), (3), or (4) is fulfilled without fulfilling criterion (1), the failure mode could be considered risky because of partial risk.

4 A Case Study from the Banking Sector

In 2021, after several discussions with compliance experts from the Hungarian retail banking sector, a workshop was organized to test the above-proposed PRISM methodology's usability on actual data. Based on real-life non-compliance cases given by the bank experts, researchers have proposed the first version of the scales of the assessment of FMEA factors and a list of the selected compliance incidents.

Based on the workshop discussion, the proposed scales of the assessment were modified, and participants have come to a common understanding. The resulting 4-grade scales in all three rating factors (occurrence, severity, and detection) are shown in Tables 6, 7 and 8.

Table 6

Ratings for the occurrence

Probability of failure	Possible failure rates	Rank
High	weekly	4
Moderate	monthly	3
Low	yearly	2
Remote	less often than once a year	1

Table 7
Ratings for the severity

Effect	Criteria: severity of the effect	Rank
Major	Severe financial, reputational or legal consequences.	4
Significant	Significant financial loss or reputational impact, legal consequences.	3
Moderate	Small financial loss, slight negative reputational impact.	2
Low	No or minor financial loss, no reputational impact.	1

Table 8
Ratings for the detection

Detection	Criteria: the likelihood of detection by the design control	Rank
Absolute uncertainty	Design control does not detect a potential cause of failure or subsequent failure mode, or there is no design control.	4
High	Internal control detects the potential cause of failure or subsequent failure mode	3
Moderate	The second line detects the event.	2
Low	Management control detects the potential cause of failure or subsequent failure mode	1

Experts set that corrective actions have to be launched if the RPN value reaches 20 points of the maximum amount of 64 points. In the next step, the experts determined that two significant outcomes can be proposed based on the risk matrices, as shown in Figure 4. The matrices' grey cells indicate the necessity of corrective actions since the partial risk is high; the white cells indicate low partial risk, so no corrective action is required.

During the workshop, three compliance experts have rated six compliance events individually. All the chosen compliance risks represent human risks. In each case, the bank clerk does not make the right decision in a given situation. By doing so, there is a compliance risk as a result of a wrong decision. Based on a discussion, following the individual ratings, a joint rating was created, as shown in Table 9.

Table 9
Compliance risks in FMEA

Case	Function/ Process step	Potential failure mode	Potential effects of failure	S	Potential causes of failure	O	Current process controls	D
A	cash withdrawal in a bank branch	a young person accompanies the elderly customer	client losing wealth	3	the client is forced to withdraw cash	2	make sure of the client's intentions	4
B	looking into client accounts	checking acquaintance's account after a phone call on business mobile	protocol violation	1	negligence or ignorance of protocols	4	random call controls, managerial controls of account lookups	3
C	replying to a customer inquiry about account abuse	customer misinformation, lack of reporting to bank security	client losing wealth, security incident	2	negligence or ignorance of internal procedure	2	employee training	4
D	cash withdrawal, account closing	the legal representative of a minor client withdraws the full amount and closes the account	minor client losing wealth	2	negligence or ignorance of internal procedure, incomplete internal procedure	1	protocols for checking personal documents	4
E	new account opening	Bank clerk opening a new account for a family member	conflict of interest, protocol violation	1	negligence or ignorance of protocols	3	managerial control	2
F	offering travel insurance	lack of reporting foreign card use	credit card abuse	2	missing protocol	4	none	4

The six cases' risk can be ranked by the RPN value, based on the multiplication of the occurrence, severity and detection values, as shown in Table 10. The higher the RPN value of a particular failure mode, the lower the ranking value.

Table 10
Risk Priority Number values of the compliance cases

Case	Occurrence (O)	Severity (S)	Detection (D)	RPN	Rank
A	3	2	4	24	2
B	1	4	3	12	4
C	2	2	4	16	3
D	2	1	4	8	5
E	1	3	2	6	6
F	2	4	4	32	1

The risk matrices in Figure 4 display the partial risks based on the three different contexts: “occurrence vs. severity”, and “occurrence vs. detection”, and “severity vs. detection”.

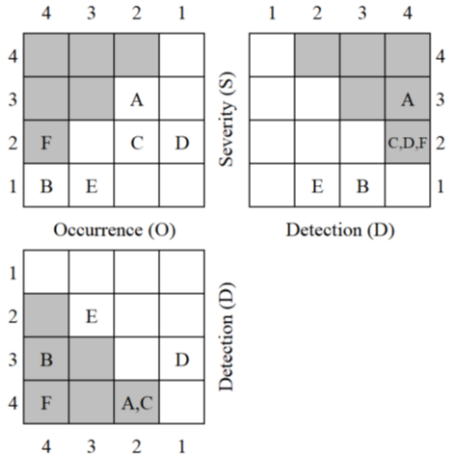

Figure 4
The PRISM pattern of the cases

Based on the RPN values and the PRISM pattern, a detailed risk assessment can be executed. As a result of the assessment, it is evident that "Case F" is the riskiest case since it has the RPN value above the previously set limit. At the same time, and it is represented three times in the PRISM pattern. "Case A" also reaches the previously set limit of the RPN value, and it is represented two times in the PRISM pattern. Though "Case C" does not reach the RPN limit, it still appears two times in the PRISM pattern, so it is necessary to launch corrective action in this case as well. "Case B" and "Case D" are under the RPN limit, but both of them are represented in the PRISM pattern once, so corrective action has to be performed in their case as well. "Case E" is under the RPN limit, and it has no appearance in the PRISM pattern. Therefore, this is the only case where no corrective action is needed.

Table 11
The detailed results of the PRISM analysis

Case	Corrective action required based on the RPN value	Corrective action required based on the PRISM pattern
A	x	x
B		x
C		x
D		x
E		
F	x	x

Table 11 summarises the required corrective actions for reducing the risk level in each compliance case. After the corrective actions were applied, a new risk assessment is performed to identify the failure modes' risk reduction.

Discussion

In the PRISM methodology, the traditional RM is applied to estimate the partial risks related to the failure modes' occurrence and severity. Simultaneously, two modified RM is also applied to estimate the occurrence and detection-based partial risks and the severity and detection-based partial risks. It is unequivocal that the three rating factors of the traditional FMEA applied in the PRISM methodology. Additionally, PRISM can also create an RPN-based ranking of different failure modes.

PRISM methodology can be interpreted as a combination and extension of the RM and FMEA. The methodology aims to describe the partial risks, which would stay hidden if only the FMEA or RM were applied. Thus, the methodology gives a more efficient and detailed view of the risk assessment result, which can be necessary for compliance sensitive and safety requiring systems. Based on the RPN values and the possibly existing partial risks, risk reductive action plans can be designed and launched.

Users can customize the PRISM methodology to the assessment's objective area, and PRISM can be useful when the corrective actions' focus has to be defined. Since partial risks can be identified as a result of the assessment, a more detailed risk-reduction action can be formed.

The PRISM methodology is a hybrid methodology that builds on the essential characteristics of the FMEA and the RM methodologies. Based on the parametrization, PRISM can be applied as a methodology that builds more to the RPN value during the risk assessment or focuses more on partial risks. Thus, the methodology can be extensively customizable to fulfil the user needs.

For example, Figure 5 shows customization options for the RPN focused risk assessment (a) and for the partial risk-focused risk assessment (b) as well.

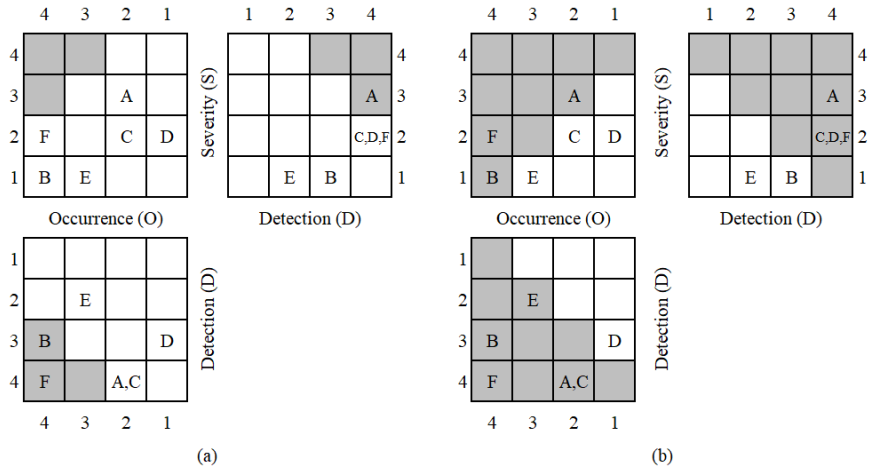

Figure 5
Customisation of the PRISM methodology

As visible in Figure 5, the customization's critical factor is the grey cells' pattern, indicating high partial risk. Case (a) shows an example where the grey cells are involved only around the rating factors' highest values. In this case, the RPN based risk assessment has more impact on the PRISM analysis. Case (b) shows an example where the grey cells have a significantly more extensive pattern than in case (a). In this case, the partial risk-based assessment has more impact on the PRISM analysis result.

The direction of the corrective actions can be set based on the position of a particular risk. The fact that the partial risk reaches the threshold at one or more part of the PRISM indicates the direction of the action plan. The most significant advantage of PRISM over the FMEA or RM is that PRISM directs the focus on those cases where the partial risk is high, but the entire RPN is low. In this case, a relatively small increase of a relatively small value of an assessment factor can result in a dangerously high overall risk, resulting in serious outcomes, especially in risk-sensitive sectors.

It is unequivocal that the PRISM methodology can apply more and different corrective action categories as well. In this case study, only two resulting categories were defined: "necessity of corrective action" and "no corrective action required". However, in other cases, more warning labels can support a detailed and more sensitive action plan.

Authors note that PRISM analysis can be performed without taking into account the RPN values. In this case, the added value of the FMEA methodology during the risk assessment process is that the PRISM methodology uses the “detection” rating factor of the traditional FMEA.

Conclusions

As a result of ever-changing external regulations and internal development, compliance nowadays appears as a specific problem. In the latest guidelines, like ISO 19600:2014, risk management and compliance management integration is highlighted.

The traditional FMEA methodology is applied to identify and assess potential or existing failure modes' risks, estimating the severity, occurrence, and ease of detecting specific failure modes. Based on the RPN value, the failure modes can be prioritised to find the riskiest ones. Corrective actions based on FMEA aim to reduce the risks. Furthermore, risk matrices apply two rating factors, which usually estimate the "occurrence" and the "severity" dimensions. Both FMEA and RM methodologies are powerful risk assessment tools.

This paper has introduced the notion of partial risk and the new PRISM methodology that combines and exceeds both the FMEA and the risk matrix's strengths, creating a new, more robust, and practical methodology. Partial risk maps can lead to a better understanding of partial risks and serve as a basis for preventive and corrective actions.

In this paper's case study, a list of compliance incidents was rated on three factors: the occurrence, severity, and ease of detection. The traditional scales have been tailored based on discussion with financial sector compliance experts.

The PRISM methodology gives a more efficient and detailed view of the risk assessment, which can be necessary for compliance-sensitive and safety-requiring systems. Based on the parametrization, PRISM can be easily customized to focus more on the RPN value or focus more on partial risks. Users can apply more and different corrective action categories (like installing alarms, training personnel, updating processes) to support a more detailed and sensitive action plan.

References

[1] Kecskés, A. (2010): Tendencies of Corporate Governance Development, Concepts of Regulation in Europe and the United Sates, PhD Thesis, https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/kecskes-andras/kecskes-andras-vedes-tezisek.pdf, pp. 20-21, 22/01/2021

[2] Paine, L. S. (1994): Managing for Organizational Integrity, Harvard Business Review, v72 n2 p106-17 Mar-Apr 1994

[3] Trevino, Weaver, Gibson, Toffler (1999): Managing Ethics and Legal Compliance, what works and what hurts, California Management Review, Vol. 41, No. 2, Winter 1999, pp. 131-151

[4] The Turner Review, a regulatory response to the global banking crises, Financial Services Authority, March 2009, http://www.fsa.gov.uk/pubs/other/turner_review.pdf, p.79-80

[5] Silverman, M. (2008): Compliance management for Public, Private, and Nonprofit Organizations, Mc Graw Hill

[6] Tarantino, A. (2008): Governance, Risk and Compliance Handbook, John Wiley & Sons

[7] Murphy, D. E. (2002): The Federal Sentencing Guidelines for Organizations: A Decade of Promoting Compliance and Ethics, Iowa Law Review, 87, 697-719

[8] The Federal Sentencing Guidelines for Organizations, chapter 8, https://www.ussc.gov/guidelines/2018-guidelines-manual/annotated-2018-chapter-8, 14/02/2021

[9] Sarbanes-Oxley Act (2002), Public Law 107–204—July 30, 2002, https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf, 14/02/2021

[10] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, 2007, https://www.sec.gov/rules/interp/2007/33-8810.pdf, 14/02/2021

[11] COSO Internal Control – Integrated Framework, 2013, https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf, 14/02/2021

[12] McNally, J. S. (2013): The 2013 COSO Framework & SOX Compliance, https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf, 14/02/2021

[13] Benedek, P. (2019): Compliance menedzsment a pénzügyi szolgáltatásokban, Munkaügyi Szemle, 62 : 4 pp. 41-51, 11 p.

[14] Coppola, F. (2018): Why The U.S. Treasury Killed A Latvian Bank, Forbes, https://www.forbes.com/sites/francescoppola/2018/02/28/why-the-u-s-treasury-killed-a-latvian-bank/?sh=76bd5d627adc, 22/01/2021

[15] ISO 31000:2018 Risk management — Guidelines, foreword, 2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 14/02/2021

[16] ISO 31000:2018 Risk management — Guidelines, foreword, 2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 14/02/2021

[17] IEC 31010:2019 Risk management — Risk assessment techniques, 2019, https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-2:v1:en,fr, 14/02/2021

[18] Naden, C. (2019): Understanding Risk with Newly Updated International Stadard, https://www.iso.org/news/ref2403.html, 08/01/2020

[19] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018, https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en, 14/02/2021

[20] ISO 19600:2014 Compliance management systems — Guidelines, 2014, https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en, 14/02/2021

[21] ISO 19600:2014 Compliance management systems — Guidelines, 2014, https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en, 14/02/2021

[22] Liu, H.C., Liu, L., Liu, N.: Risk evaluation approaches in failure mode and effects analysis: A literature review. Expert Systems with Applications 40 (2013) 828-838

[23] Liu, H. C., Chen, X. Q., Duan, C. Y., Wang, Y. M.: Failure mode and effect analysis using multi-criteria decision making methods: A systematic literature review. Computers & Industrial Engineering 135 (2019) 881-897

[24] Chen, L., Deng Y.: A new failure mode and effects analysis model using Dempster–Shafer evidence theory and grey relational projection method. Engineering Applications of Artificial Intelligence 76 (2018) 13-20

[25] Song, W., Li, J., Li, H., Ming, X.: Human factors risk assessment: An integrated method for improving safety in clinical use of medical devices. Applied Soft Computing Journal 86 (2020) 105918

[26] Chang, K. H.: Evaluate the orderings of risk for failure problems using a more general RPN methodology. Microelectronics Reliability, 49 (2009) 1586-1596

[27] Chang, K. H., Cheng, C. H.: A risk assessment methodology using intuitionistic fuzzy set in FMEA. International Journal of Systems Science, 41 (2010) 1457-1471

[28] Liu, H. C., Liu, L., Liu, N., & Mao, L. X.: Risk evaluation in failure mode and effects analysis with extended VIKOR method under fuzzy environment. Expert Systems with Applications, 39 (2012) 12926-12934

[29] Sankar, N. R., & Prabhu, B. S.: Modified approach for prioritization of failures in a system failure mode and effects analysis. International Journal of Quality & Reliability Management, 18 (2001) 324-336

[30] Seyed-Hosseini, S. M., Safaei, N., & Asgharpour, M. J.: Reprioritization of failures in a system failure mode and effects analysis by decision making trial and evaluation laboratory technique. Reliability Engineering & System Safety, 91 (2006) 872-881

[31] 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

[32] Wang, R., Wang, J.: Risk Analysis of Out-drum Mixing Cement Solidification by HAZOP and Risk Matrix. Annals of Nuclear Energy, 147 (2020) 107679