HABILITATION THESES BOOKLET

Quality-Oriented Compliance Management

Petra Benedek, PhD
assistant professor
Budapest University of Technology and Economics
Faculty of Economic and Social Sciences
Department of Management and Business Economics

Budapest
2025

Contents

List of Tables

List of Figures

Quality-oriented compliance management

In this document, I would like to present my professional work and scientific results in the field of management and organizational sciences since obtaining my PhD degree. First, I will formulate my habilitation theses. Next, will explain in detail the scientific results related to the habilitation theses along the selected articles. Finally, I will outline the main directions of my future scientific research and practical application possibilities.

Background and description of the theses

In the past three decades, the extent of regulatory changes has led to their compliance becoming an independent management task. Similar to the broadly interpreted internal control system, compliance management also dynamically adapts to the expectations of the company's operating environment. The quality management system, compliance management, and risk management are all functions supporting the internal control system. Their relationship is unique for each organization and is constantly changing. Even within a given industry, each actor interprets the requirements that determine their business activities independently.

While nonconformity (or deviation), a term regularly used in quality management, refers to the failure to comply with an organization's external or internal regulations, procedures, or quality standards, noncompliance refers to the failure to comply with laws, regulations, or external standards. Both terms refer to the failure to comply with requirements or obligations, but nonconformity (regulations/standards) is more internal, while noncompliance is typically external (laws/regulations), although there is overlap between the two, and the boundary is not considered sharp. Nonconformity and noncompliance often go hand in hand and may be causally related. For example, in the case of a university, the improper handling of student data is likely to be a deviation from the institution's internal regulations and also a violation of the GDPR or other data protection laws. Deviation from internal regulations does not necessarily mean external irregularity, but in the opposite case, both typically occur simultaneously. It follows from the above that compliance (legality, regularity) is a fundamental element of the quality of processes, both in terms of the regular production of products and legally regulated product characteristics (e.g., harmful substance content), and the legal, regular provision of services and regulated service characteristics.

My habilitation theses are related to four selected articles. In the order of discussion, they are as follows:

1. Bognár, F., Benedek, P. (2021). Case Study on a Potential Application of Failure Mode and Effects Analysis in Assessing Compliance Risks. Risks, 9(9), 164. https://doi.org/10.3390/risks9090164
2. Bognár, F., Szentes, B., Benedek, P. (2023). Compliance Risk Assessment in the Banking Sector – Application of a Novel Pairwise Comparison-based PRISM Method. Complexity, Paper: 9165815, https://doi.org/10.1155/2023/9165815
3. Benedek, P., Surman, V. (2025). Compliance QFD – how compliance contributes to quality in higher education. Educational Research and Evaluation, 30(5–6), 345–368. https://doi.org/10.1080/13803611.2024.2437425
4. Benedek, P., Bognár, F. (2024). Compliance Risk Assessment - Results of a Comprehensive Literature Review. Acta Polytechnica Hungarica 21(6), 243-262. https://doi.org/10.12700/APH.21.6.2024.6.13

T1: I extended the application of the Failure Mode and Effects Analysis (FMEA) method, often used in quality management, to the field of compliance management. By introducing the detection factor, I developed a compliance risk assessment method that goes beyond traditional risk maps.

T2: I have further developed the Partial Risk Map (PRISM) methodology for compliance risk assessment. The PRISM method has the advantage of visualization, offering a more detailed and nuanced risk ranking that supports managerial decision-making. This methodology enables the more efficient allocation of risk mitigation resources by drawing attention to hidden risks.

T3: By adapting the QFD process, I have created a compliance-specific QFD process that translates stakeholder expectations into quality-oriented compliance objectives. I have applied this method in higher education to assess how regulatory compliance and compliance operations affect customer satisfaction, primarily that of students. My approach provides a strategic tool for aligning compliance activities with stakeholder expectations, ultimately increasing service quality and thereby stakeholder satisfaction.

T4: I have proposed a definition of compliance risk. According to the definition, compliance risk refers to an event with the likelihood of potential regulatory, financial, or reputational losses for the organization due to noncompliance with regulations or voluntary obligations.. I have developed a structured, three-step compliance risk assessment process. The first step is to identify compliance risks, the second step is to analyze compliance risks (analyze the likelihood and impact of noncompliance and assess their detectability under current controls), and the third step is to evaluate risk (rank the risks). The structured compliance risk assessment process ends with a decision. The five possible outcomes of the decision are: the organization avoids, accepts, transfers or reduces the risk, or increases it to exploit business opportunities.

T5: Quality and compliance management are complementary management areas, where compliance ensures compliance with laws and other regulations, and thereby contributes to quality improvement. An integrated approach to the two areas can lead to more efficient resource use and better business/organizational results. Through my theoretical and empirical research, I have demonstrated how compliance can stimulate quality improvement, contributing to the achievement of strategic goals.

Presentation of scientific results leading to the theses

My goal is to present in a unified way how the individual articles contributed to the habilitation theses. In each subsection, I briefly describe the purpose of the article, present the methodology and results, and their novelty. Finally, I connect the content of the given subsection with the habilitation theses.

Application of FMEA to assess compliance risks

This subsection presents the contribution of my work, Bognár, F., Benedek, P. (2021). Case Study on a Potential Application of Failure Mode and Effects Analysis in Assessing Compliance Risks. Risks, 9(9), 164. https://doi.org/10.3390/risks9090164. In this subsection, I present the application of the FMEA method to the field of compliance management. By introducing the detection factor, I have developed a compliance risk assessment method that goes beyond traditional risk maps.

The study presents the results of exploratory research based on the application of FMEA at a commercial bank in Central and Eastern Europe. Banks are considered "dangerous" operations due to the several risks they face, which are much higher than those of other business actors. The control functions, described as the first, second, and third lines of defense since 2013 based on a recommendation published by the Institute of Internal Auditors (IIA, 2013), protect the organization while actively and proactively supporting the business/operational areas. The "three-line model", which was significantly updated by the Institute of Internal Auditors in July 2020, focuses on the supporting function and risk management. (IIA, 2020)

While failure mode and effects analysis (FMEA) is widely used in industrial settings, its application in the financial sector is novel. The traditional FMEA method was created in the 1960s, essentially as a tactical risk analysis methodology. The purpose of FMEA is to assess risks, usually for a product or process, and then reduce them through action plans (Huang et al., 2020). Traditional FMEA is a group method that builds on group assessments that emerge during collective discussions of group members.

The primary motivation for this study was to describe a methodological process that can lead compliance experts to agree on the prioritization of risks by statistically monitoring the level of agreement.

The research question was: Can an FMEA-based compliance risk assessment process be developed that also monitors the level of group agreement? In this study, I examined two hypotheses:

> Assumption 1. By using FMEA as a nominal group technique, differences can be detected between organizational expert assessments.
> Assumption 2. By using FMEA as a nominal group technique, it can be shown that experts within a given organization assess risks similarly to each other, but differently compared to an external expert.

I conducted the data collection at one of the largest commercial banks in Central and Eastern Europe in January 2021. The focus group consisted of six participants – three compliance experts from the commercial bank's headquarters, one external compliance expert, and two moderators. The selected banking experts had to meet the following criteria: they had to have more than ten years of experience in the banking sector in the field of compliance management,

and more than five years of experience at the current bank. On the other hand, the external expert had to have in-depth regulatory knowledge and general compliance experience, but little understanding of the bank's specific internal processes, compliance management system, and philosophy. The steps of the empirical research are presented in Figure 1.

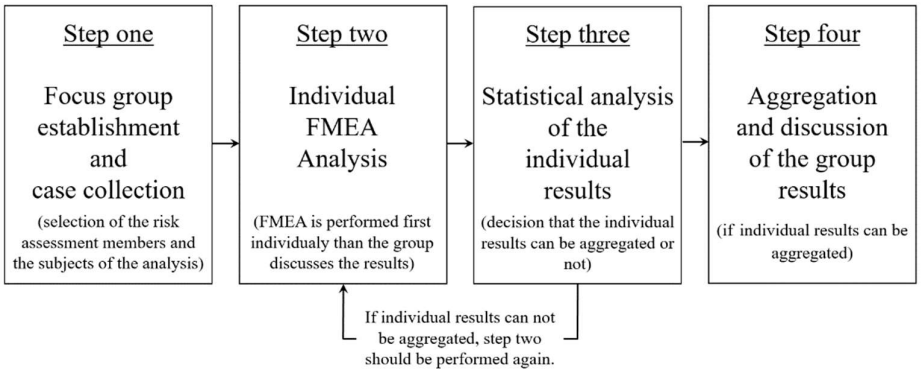


Figure 1. The process of empirical research
Source: Bognár, Benedek, 2021, p. 8.

Before the workshop, I asked the bank to collect compliance risks. We identified the risks that arise in the administration of the bank branch. In each case, the focus was on the bank administrator not making the right decision in a given situation, thus creating a compliance risk due to the wrong decision. Out of a total of thirty cases provided by the bank, I selected six cases for analysis. The methodology would be the same if there were more or fewer cases. The risk assessment of the randomly chosen cases was the task of the four experts. Due to the length of the description of the six risky cases, I will not present them here.

In recent decades, a broad theoretical consensus has emerged in the research community about which scales are worth using to assess certain dimensions of risk assessment (Liu et al., 2013). Still, in practice, the scales are often modified. In this case, the participants used four-point scales with a previously agreed interpretation to capture the probability of occurrence, the severity of the consequence, and the difficulty of detection. Risk can be calculated as the product of the three factors, so in our case, the risk index (Risk, Priority Number, RPN) can therefore range from 1 to 64.

During the focus group workshop, the experts carried out the risk assessment individually, independently of each other, i.e., as a nominal group. In the process, the experts assessed the six cases according to the three previously defined scales. I aggregated the individual results in two ways. In one case, I took into account the results of all four experts, and in the other case, only the results of the bank's internal compliance experts. The aggregation method was simple arithmetic averaging.

Furthermore, by transforming individual expert assessments to an ordinal measurement level, i.e., forming rankings, individual expert opinions and group expert opinions can be professionally compared and examined. The statistical examination of the rankings made it clear how similar the individual expert assessments are.

I present the results according to the research assumptions. According to the first assumption, differences can be detected between organizational expert assessments by using FMEA as a nominal group technique. I transformed the organizational expert assessments into rankings and examined them using Spearman rank correlation and Kendall rank concordance coefficients.

Table 1 shows the results of the Spearman rank correlation analysis. The value of the Spearman rank correlation coefficient is between 0 and 1 for all expert comparisons, and only in one case, in the judgment of detection shows difference at a 5% significance level. This case is highlighted in gray in Table 1.

Table 1: Rank correlations when examining the evaluations of organizational experts
Source: Bognár, Benedek, 2021, p. 10.

Expert vs expert	S		O		D		RPN	
	Spearman rho	Significance level	Spearman rho	Significance level	Spearman rho	Significance level	Spearman rho	Significance level
Compliance expert 1 vs. 2	0.850	0.032	0.874	0.023	0.900	0.015	0.971	0.001
Compliance expert 1 vs. 3	0.900	0.015	0.907	0.013	0.904	0.013	0.886	0.019
Compliance expert 2 vs. 3	0.900	0.015	0.820	0.046	0.710	*0.114*	0.912	0.011

The Kendall W rank concordance values, which examine the similarity of the three assessments, fluctuate around 0.9 and are significant at the 5% significance level in all cases. In case of substantial differences, aggregating the assessments would not yield reliable results; however, in this case, the assessments can be aggregated.

According to the second assumption, by applying FMEA as a nominal group technique, it can be shown that experts of a given organization evaluate risks similarly to each other, but differently compared to an external expert. Similarly to the previous ones, I calculated the Spearman's rank correlation values taking into account the external expert. Examining the external expert, Spearman's rank correlation value is between 0 and 1 in all cases, but only in one case does it show significant similarity at the 5% significance level of the results. This case is highlighted in Table 2.

Table 2: Rank correlations when examining the evaluations of all experts
Source: Bognár, Benedek, 2021, p. 11.

Expert vs expert	S		O		D		RPN	
	Spearman rho	Signifi-cance level	Spearman rho	Signifi-cance level	Spearman rho	Signifi-cance level	Spearman rho	Signifi-cance level
Compli-ance ex-pert 1 vs. External expert	0.617	0.192	0.783	0.065	0.302	0.561	0.371	0.468
Compli-ance ex-pert 2 vs. External expert	0.867	*0.025*	0.420	0.407	0.254	0.627	0.441	0.381
Compli-ance ex-pert 3 vs. External expert	0.767	0.075	0.718	0.108	0.369	0.471	0.486	0.329

Table 3 shows the results of the Kendall rank concordance analysis, which I calculated for the rankings of the external expert and the bank compliance experts.

Table 3: Kendall W values for the external and organizational expert rankings
Source: Bognár, Benedek, 2021, p. 11.

Evaluation	Kendall W	Significance level
S	0.863	0.004
O	0.819	0.006
D	0.676	0.019
RPN	0.757	0.010

For the four rankings created with the involvement of the external expert, the Kendall W values are significant at the 5% significance level. The Kendall rank concordance values decreased with the participation of an external expert; for example, the RPN decreased from 0.948 to 0.757. Since the Kendall W values are sufficiently high, the assessment results of the bank's compliance experts can be aggregated.

The examination of group-level agreement shows that the agreement between the bank's experts is significant. In terms of decision support, the Kendall rank concordance coefficient provides more detailed information.

The tables created for assessing compliance risks, assessing severity, occurrence, and perception, are sufficiently good descriptors of the risk levels, and the experts see the risks underlying each case similarly. The risk assessment methodology based on the nominal group technique, in which participants independently perform the risk assessment, provides feedback on the agreement, which cannot be measured in the case of traditional joint assessment. I investigated whether the independent expert opinions differ too much from each other, since in case of significant differences, averaging the assessments would not give reliable results.

A further conclusion is that the external expert sees compliance risks significantly differently. This finding is supported by a pairwise comparison of the rankings of the external expert and

the organizational experts, which resulted in significantly similar rankings in only one case. In this regard, it can be stated that the method can distinguish experts based on their knowledge.

The added value of FMEA compared to risk matrices is the perception factor. In our example, the only non-significant result among the organizational experts' assessments occurs when using the detection ranking factor (Table 1). On the other hand, the most significant difference between the organizational and external experts' assessments is in the perception ranking (Table 2). This result highlights the relative importance of using the perception factor and FMEA instead of risk matrices, as the perception rating factor summarizes a lot of information that is worth considering during the assessment.

Of the three FMEA factors, frequency of occurrence and severity of consequences are widely used dimensions in risk matrices. One important novelty of the application of FMEA in the financial sector is that it raises the detection of failures to the same level of importance as other assessment dimensions. If available data supports the assessment of FMEA factors (for example, frequency or time series data), this can provide an even better basis for decision-making.

Different experiences and incentives can cause significant differences in the way individual experts assess risks, from assessing the operational context to the events that occur. A comparative analysis of expert assessments can provide information about the lack of specialized knowledge or experience. Alternatively, it can reveal new perspectives, draw attention to new issues, and contribute to a better understanding of the organization's risk exposure. Individual assessment of risks can be supplemented in this process by subsequent group discussion of the results.

Contribution of the subsection to the individual habilitation theses

- I have presented the application of the FMEA method to the field of compliance management.
- I have applied the FMEA as a nominal group technique, allowing for a systematic comparison of individual and group assessments.
- Individual, independent expert assessments can identify those differences that may be due to a lack of knowledge or a new perspective on risk exposure. Applying the methodology can reveal new insights, especially when assessments differ significantly.
- It provides an opportunity for expert groups to test consensus.
- FMEA-based risk assessments are effective in monitoring group-level agreements on compliance risks, as successive FMEA analyses can be compared over time, thus capturing changes.
- I assign the article to theses T1 and T5.

Application of the PRISM Methodology to Compliance Risk Assessment

This subsection presents the contribution of my work, Bognár, F., Szentes, B., Benedek, P. (2023). Compliance Risk Assessment in the Banking Sector – Application of a Novel Pairwise Comparison-based PRISM Method. Complexity, Paper: 9165815, https://doi.org/10.1155/2023/9165815. In this subsection, I present the application of the Partial Risk Map method to the field of compliance management. The PRISM method has the advantage of visualization and offers a more detailed and nuanced risk ranking than the RPN values of FMEA. The method supports a more efficient allocation of risk mitigation resources by drawing attention to hidden risks.

The scope and activities of compliance are increasingly complex, necessitating the development of risk assessment processes to keep pace with this complexity. Risk matrices and failure mode and effects analysis (FMEA) have been developed in many industries as risk assessment techniques in recent decades. (Liu et al., 2013) As a new risk assessment technique based on FMEA factors, the PRISM method focuses on the assessment of partial risks that remain hidden but lead to potentially serious impacts (Bognár, Benedek, 2021). As several studies have shown (Losiewicz-Dniestrzanska, 2015, Bezrodna, 2019, Salvioni et al., 2016, Naheem, 2019), assessing banking compliance risk is a significantly complex process that includes many different assessment factors. Hidden risks in banking compliance management can seriously damage the reputation of the organization, and the spillover effects can pose an additional threat to the entire sector (Eckert, Gatzert, 2019).

In 2021, the International Organization for Standardization (ISO) published a new standard, ISO 37301:2021 Compliance management systems – Requirements with guidance for use, which supersedes the first international guideline on compliance management (ISO 19600:2014). The most significant change is the shift from guidelines to requirements, along with the possibility of certifying CMS by the standards. Although not explicitly stated, governance, risk, and compliance (GRC) is the dominant approach in the ISO 37301:2021 standard. The standard requires organizations to maintain documented information on compliance risk assessment, nonconformity records, and investigations.

In the standard, risk identification is linked to the Plan phase, mitigation through controls and procedures to the Do phase, and measurement and monitoring activities to the Check phase of the PDCA cycle. The standard, therefore, requires risk identification and quantification based on risk assessment methodologies, with prevention in mind. Risk identification generally describes the following characteristics of the risk: its nature, source, and impact, e.g., event, business line, regulatory consequence. (AIRMIC, 2010) In practice, compliance risk management is primarily based on consultations with expert groups, while the reliability of these consultations is rarely examined. Risk management and mitigation aim to reduce the likelihood and negative impact of risky events. The implementation of risk mitigation measures is prioritized and scheduled due to the availability of professional and financial resources.

This article aims to present a new risk assessment technique, based on a case study, that is not scale-based, can be used to test the consistency of evaluators, and the similarities and differences of the results of evaluators can be compared in detail with each other, thereby reducing the uncertainty of group decision-making.

Data collection took place within the framework of the focus group presented in the previous subsection, with the participation of the three bank compliance experts. The experts evaluated

the compliance cases three times, using the Guilford pairwise comparison method, according to the factors of occurrence, severity, and ease of detection. The results of the experts' consistency test showed that Experts 1 and 2 were consistent in the comparisons based on occurrence, severity, and perceptibility. In contrast, expert 3 was consistent only in the comparison based on severity. Therefore, when aggregating the severity assessment, I took into account the assessments of three experts, while for the other two factors, I took into account the assessments of two experts.

Next, I highlight those parts of the selected article that go beyond the methodology presented in the previous subsection. The PRISM method, based on Guilford's pairwise comparison, goes beyond the application of previously agreed (four-point or ten-point) scales (FMEA dimension tables). Furthermore, the combination of the PRISM method with pairwise comparison methods allows for testing the consistency of experts' thinking. At the same time, this possibility was not yet present in the original PRISM method (Bognár, Benedek, 2021b) and is also new in compliance risk assessments. Thus, thanks to pairwise comparison, the rationality of the thinking of individual assessors, i.e., the consistency of their thinking, can be examined. Excluding inconsistent experts from the aggregation leads to more accurate results in the rest of the assessment process.

The subsequent significant development is visualization. By imagining the three factors that make up the RPN number calculated in the FMEA in space and selecting any two of the three factors, the risks can be represented in two dimensions. The PRISM method, therefore, displays three projections of the RPN "cube" by omitting one factor. For each projection, we examine the value of the risks separately, which are partial risks. In Figure 2, all six risks are included in all three partial risk maps (C1-C6).

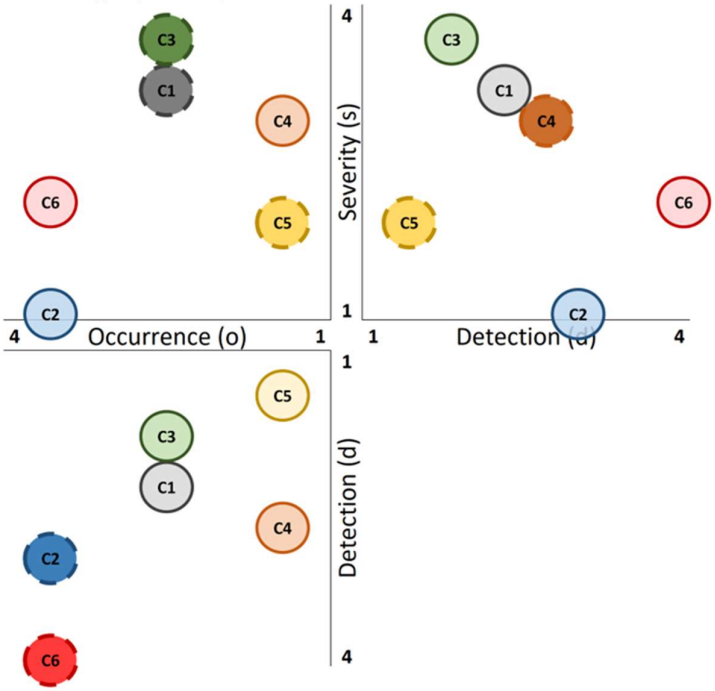


Figure 2: Illustrating risks on the PRISM map
Source: Bognár et al., 2023, p. 9.

Based on the results, C6 has the highest relative partial risk, which is the riskiest case. Since this is the highest partial risk in the occurrence vs. detection submatrix, the possible risk mitigation strategy is to reduce the probability/frequency or increase the detectability. All

consistent experts agreed that C5 is the least risky case. Since only significantly consistent experts participated in the aggregate assessment and the individual assessments were similar, it can be concluded that the evaluation is based on adequate knowledge and the results are reliable.

According to the standard practice at the given bank, only four outputs are used for the outcome of the risk assessment (mild, moderate, significant, and critical), so many problems have the same output rating. In cases of scarce resources, there is no information on which problem with the same output value should be prioritized for mitigation. By applying the proposed PRISM method, the ranking will be more detailed. In the case of identical RPN values, the PRISM map can illustrate the combination of factors that formed the RPN value, so that the differences between the risk factors can be captured, and this information can be used in managerial decision-making.

Contribution of the subsection to the habilitation theses:

- I have further developed the partial risk map (PRISM) methodology to fit compliance risk assessment.
- The advantage of the presented method is visualization, offering a more detailed and nuanced risk ranking, which supports managerial decision-making.
- The methodology draws attention to hidden risks and, in the case of identical RPN values, provides insight into the characteristics of the assessment factors. The new method helps to allocate risk reduction resources more efficiently by clearly ranking risks of similar RPN value.
- Thanks to the pairwise comparison, the rationality of the thinking of individual assessors can be examined, and the exclusion of inconsistent experts from the aggregation leads to more accurate results. Combining PRISM and Guilford pairwise comparisons increases reliability in complex risk assessments.
- Predefined scales limit the ability to distinguish between similar risks, reducing the effectiveness of prioritization. The PRISM method, based on Guilford's pairwise comparisons, goes beyond the use of pre-agreed scales.
- I assign the article to theses T2 and T5.

Compliance QFD

This subsection presents my work entitled Benedek, P., Surman, V. (2025). Compliance QFD – how compliance contributes to quality in higher education. Educational Research and Evaluation, 30(5–6), 345–368. https://doi.org/10.1080/13803611.2024.2437425. In this subsection, I present the birth of the concept and procedure of the compliance QFD.

The methodology is essentially an adaptation of the Quality Function Deployment (QFD) method used in quality management to the field of compliance, and in this case, it was designed to develop higher education as a service. According to Becket and Brookes (2008), the traditional quality management practice of higher education institutions is typically based on the PDCA process. While quality assurance in higher education is an established research area, the contribution of compliance management to maintaining or improving the quality of higher education is a novel research area. In Hungary, the transformation of higher education institutions further strengthens the need to focus on performance evaluation and meeting stakeholder expectations (Nagy and Somosi, 2020), so the study can be considered timely and relevant from a practical perspective.

The aim of the publication is to present a development concept and framework, a so-called quality framework (QFD), to improve the service quality of higher education institutions. The development of Compliance QFD builds on previous work by Surman and Tóth (Surman and Tóth, 2021; Surman, 2021; Surman et al., 2022), in which questionnaire surveys and focus group interviews were conducted to determine service quality attributes (SQAs). Although the SQAs that can be interpreted at the institutional level in higher education are similar worldwide, the list used in the research is mainly based on the expectations of Hungarian students towards domestic higher education institutions.

The aim of the publication is to examine the service quality elements defined by Surman et al. (2022) related to the institutional level of higher education institutions from the perspective of compliance management. The significance of the study lies in its application of the QFD method to connect service quality attributes with compliance management activities and functions in higher education institutions. The research can be considered exploratory, as a significant part of it consists of literature research, which primarily aims to identify the compliance activities of higher education institutions and the (technical) factors displayed in QFD, and then analyze the relationships.

The critical difference between compliance management and traditional quality management lies in the focus and approach. Compliance management ensures that the institution complies with external laws, regulations, and accreditation standards. It primarily aims to meet mandatory requirements imposed by governing bodies, ensure compliance with legal and regulatory obligations, and avoid sanctions and loss of accreditation. Traditional quality management is a tool for promoting a culture of continuous improvement. The organization focuses on improving the quality of education (and possibly research as a core activity) through internal reviews, feedback mechanisms, self-assessment, and compliance with external standards. In summary, compliance management ensures legal and regulatory compliance, while quality management continuously strives to improve scientific and administrative processes.

The main steps in creating a compliance QFD were identified based on the study by Hwarng and Teo (2001), which focuses explicitly on the application of QFD in services (including higher education). When applying the method (Figure 3), assessing customer needs was a critical step, as this provided the basis for the direction of development.

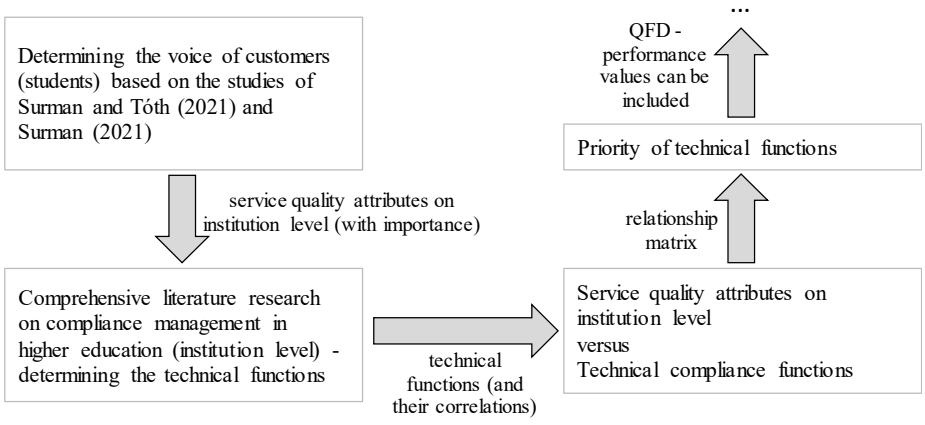


Figure 3. The compliance QFD development process
Source: Benedek, Surman, 2025

The foundational empirical research considered students as primary stakeholders, but the insights of faculty were also collected and used, as they were defined as secondary stakeholders. After mapping the stakeholders, expectations regarding service quality at the institutional level were collected and then linked to service characteristics (based on Vezzetti et al., 2016). In the article describing compliance QFD, we linked these service characteristics (VOC, Voice of the Customer) to key processes related to compliance management (Voice of the Organization, VOO), and finally ranked the compliance functions.

In QFD, compliance management functions refer to systematic activities performed by the organization. The core activities, essentially beyond the higher education sector, include:

- ensuring compliance with external regulations,
- ensuring consistency within internal regulations and coordinating them,
- providing whistleblowing procedures and channels,
- risk management to identify and mitigate potential noncompliance,
- incident management to address violations,
- communication.

In compliance QFD, these functions are the technical parameters that ensure that regulatory requirements and quality standards are integrated into processes. I have defined the technical, or in this case, compliance, functions of QFD mainly based on the ISO 37301:2021 standard and the literature listed in Table 4.

Table 4: Compliance functions
Source: Benedek, Surman, 2025

Compliance functions	**Description**	**Literature**
conformance to external regulations	planned and coordinated activities to ensure compliance with external rules and regulations, formal requirements, procedures, specifications, standards	Choi, Chun, 2021 Olt, 2020
consistency of internal regulations	consistency of controls, systems, mechanisms and methods of standard operating procedure	Jackson, 1997 Hatta et al., 2019 Romzek, Dubnick, 1987
leadership commitment	attention and resources allocated to compliance issues and activities, tolerance for rule-breaking, setting norms of behaviour	Do et al., 2017 Lipton et al., 2022
whistleblowing	providing channels for making complaints and providing protection to incident reporters	Dorasamy, 2013 Ashton, 2015 Bernardi et al., 2016
compliance communication	formal or informal requirements of communication related to ensuring compliance	Sahney et al., 2010 Hatta et al., 2019
risk management	compliance risk identification, assessment and mitigation	ISO, 2021 Bamber, 2022 Bognár. Hegedűs, 2022 Bognár, Böcskei, 2022

information use and confidentiality	data protection, codes of conduct	Alshare et al., 2018 Hatta et al., 2019 Hina et al., 2019 Bederna et al., 2021
incident management	detection, remediation and correction of noncompliances	Noda et al., 2018 Root, 2019
compliance culture	adjusting behaviour and practice to explicit or implicit rules, training	ISO, 2021 Dawson, 2009

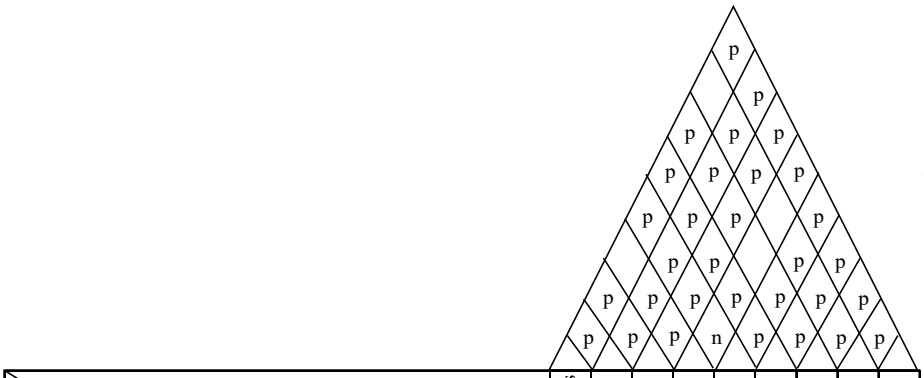
In addition to the general compliance activities listed above, I have defined a total of nine compliance functions in QFD, expanded with three additional elements. The first added function is leadership commitment. This is crucial, as it determines the overall organizational tolerance level for noncompliance. Leadership commitment is reflected in the attention and resources managers devote to compliance issues and activities. (Lipton et al., 2022).

The second added function is information use and confidentiality. The core "activity" of higher education involves the various flows of information and knowledge, while the protection of personal or sensitive data is critical. The protection of information as a resource in teaching, research, and knowledge preservation in higher education institutions is a priority area of compliance (Hatta et al., 2019).

The third added function is compliance culture. Although academia has traditionally been strong in incident detection and response, modern compliance approaches focus on preventing irregularities and creating a proactive culture. The general willingness to report incidents, the justification for reporting or not reporting, and compliance awareness also fall within the domain of culture (ISO, 2021).

The relationships between service quality attributes (VOC) and compliance functions (VOO) are contained in the central area of the quality house. Four types of relationships are distinguished: no relationship, weak relationship, medium-strong relationship, and strong relationship. Since the relationship types are to be used in the priority calculations of the compliance functions, the values corresponding to each type are: no relationship – 0, weak – 1, medium – 3, strong – 9.

After defining the VOC and VOO, the first step was to assess the possible relationships between the ten service quality attributes and the nine compliance functions. In almost all cases, a relationship of some strength could be determined (see Figure 4).



Customer needs \ Technical functions		Conformance to external regulations	Consistency of internal regulations	Leadership commitment	Whistleblowing	Compliance communication	Risk management	Information use and confidentiality	Incident management	Compliance culture
Career opportunities during the studies	3.6	3	0	1	0	0	3	0	1	3
Career opportunities after the studies	4.51	3	1	3	0	0	3	0	3	9
Lecturers' scientific work and professional reputation	4.03	1	3	3	1	3	9	3	9	9
Institutional infrastructure and equipment	3.66	3	9	9	1	1	3	3	3	9
Reliability	4.58	9	9	9	3	9	9	9	9	9
Institutional commitment towards improvement	4.53	9	9	9	0	1	3	3	3	9
Institutional reputation	3.77	3	3	3	3	1	9	3	9	9
Internationality	3.65	1	3	3	1	1	3	1	3	3
Industrial relationships	4.26	1	3	3	1	0	3	3	1	3
Application process	3.27	9	9	3	0	3	9	9	9	9
Technical priority		170	291	309	54	35	153	246	240	420

Figure 4: Compliance QFD
Source: Benedek, Surman, 2025

In the next step, I defined the relationships between the compliance functions. Compliance with external regulations supports the operation of almost all other functions, except for two, namely, whistleblowing and incident management. Since it permeates the entire operation of institutions, compliance with internal regulations also supports all other functions. The development and operation of risk management and a compliance culture have a positive effect on the operation of all other functions.

The priority values of the compliance functions are determined by simply summing the products, thus obtaining a general picture of the importance of compliance areas, primarily from the point of view of student expectations. The formula is as follows:

$$\textbf{Technical priority of } \mathbf{CF_m} = \sum \mathbf{SQA_n} * \mathbf{RM_{m,n}} \quad (1)$$

where m represents the column of the examined compliance function (CF), and n shows the row of the given service quality attribute (SQA). RM demonstrates the relationship matrix values in the given column (m) and row (n).

I calculated the priority values of the compliance functions according to Formula 1. For example, the compliance function shown in the last column, compliance culture, has a medium relationship with career opportunities offered during studies, internationality, and industrial relations. Therefore, we multiply the importance values of the above three VOC attributes by three. All other VOC attributes have a strong relationship with the compliance function; therefore, we multiply the importance values by nine. In the last column, the sum of the products results in a priority value of 420, which is the highest value in Table 5.

Table 5. Priorities of compliance functions based on compliance QFD
Source: Benedek, Surman, 2025

Compliance functions	**Priority**
Compliance culture	420
Leadership commitment	309
Consistency of internal regulations	291
Information use and confidentiality	246
Incident management	240
Conformance to external regulations	170
Risk management	153
Whistleblowing	54
Compliance communication	35

Table 5 shows the priority order of compliance functions based on the calculations. At the top of the list is a compliance-conscious culture and leadership committed to compliance and adherence to regulations. In third place is the consistency of internal regulations. Information use and confidentiality, incident management, compliance with external regulations, and risk management are in the middle, while whistleblowing and communication are at the bottom of the list.

Both traditional quality management and compliance management are essential in higher education. Together, they ensure regulatory integrity and educational excellence. The QFD method transforms customer expectations into technical parameters and defines design goals. This method is valuable in designing and implementing institutional (compliance) strategies that focus on increasing competitiveness and stakeholder satisfaction (Miguel, 2005; Yadav and Gahlot, 2022; Bugdol and Jedynak, 2022). As higher education institutions experience an increasing demand for transparent operations and face diverse stakeholder needs and expectations, compliance and quality management processes in higher education are crucial for legitimacy, funding, customer satisfaction, and competitiveness. (Bamber, 2022; Choi and Chun, 2021)

This study has shown how students' needs and expectations (VOC) can be translated into higher education institutions' compliance activities (VOO). The resulting compliance QFD highlights the importance of a compliant and aware culture and leadership commitment. However, the relationship values between SQAs and compliance functions show a general picture. In a specific application, following the process described in Figure 3, SQAs and compliance

functions can be reviewed and modified, which may also result in a change in the priority order. If compliance QFD is used explicitly for an institution, it is advisable to fill it with additional institution-specific characteristics. In this case, strategically important areas can indeed be highlighted, between which it is essential to examine the correlation (if the institution wants to develop in several areas at the same time).

Overall, the novelty of compliance QFD lies in its ability to go beyond the mere interpretation and implementation of legal requirements, and also takes into account the specific expectations of the higher education institution and its primary stakeholders, the students. The study highlights that the development of a given compliance management area will also affect service quality characteristics and other compliance functions, which can potentially increase student satisfaction and the competitiveness of the institution. One of the characteristics of the study is that it focuses on service quality at the institutional level. In contrast, quality at the program or course level was left out of this research.

Contribution of the subsection to the habilitation theses

- According to the article, both quality and compliance management are complementary areas, where compliance ensures compliance with legislation; quality management encourages continuous improvement.
- The compliance QFD method helps to translate stakeholder expectations into institutional compliance and quality goals.
- Compliance QFD highlights the importance of a compliance-sensitive, compliance-aware culture and committed leadership. Culture and leadership have a critical impact; their absence leads to operational and reputational risks.
- The new compliance QFD method developed can help an institution recognize and assess the relationship between operational compliance, rule-following, and student satisfaction.
- I assign the article to theses T3 and T5.

The Compliance Risk Assessment Process

This subsection presents the contribution of my work, Benedek, P., Bognár, F. (2024). Compliance Risk Assessment - Results of a Comprehensive Literature Review. Acta Polytechnica Hungarica 21(6), 243-262. https://doi.org/10.12700/APH.21.6.2024.6.13. In this subsection, I present the definition of the concept of compliance risk and the developed three-step compliance risk assessment process.

The study focuses on different interpretations of compliance risk and the compliance risk assessment process. I examined the following research questions:
Question 1: What meanings does the term compliance risk contain?
Question 2: What does the compliance risk assessment process look like according to the literature?
Question 3: What are the gaps in the current literature that could shape future research?

An early but frequently cited definition of compliance risk is that of an organization's exposure to potential legal or regulatory sanctions, financial loss, or reputational damage resulting from noncompliance with laws and regulations that apply to the organization (Basel Committee, 2005).

Compliance risk, therefore, primarily consists of the penalties and other consequences of regulatory noncompliance, as well as reputational risk. The former includes illegal practices such as fraud, theft, bribery, money laundering, and embezzlement. Violations of data protection laws, pollution, environmental damage, and violations of occupational health and safety regulations are also common compliance risks. Cloud computing introduces new compliance risks, as cloud services may store sensitive or proprietary data.

Another important source is the current ISO 37301:2021 standard for compliance management systems, which follows the PDCA logic. In this, the identification of risks is part of the Planning phase, the mitigation of compliance risks through controls and procedures is part of the Do phase, and the measurement and monitoring activities are included in the Check phase.

The research was based on a literature review. I used the Scopus database, which is used by many research studies to select and identify relevant studies. The selection process was based on the following keywords: compliance risk OR compliance assessment OR compliance risk evaluation. The search was conducted in July 2023 following the logic of the PRISMA 2020 statement. I extended the search to include a regulatory document outside Scopus (Basel Committee, 2005), which is cited as an essential reference point in many studies. To examine the research questions, I defined the following criteria: (i) journal articles and regulatory reports that addressed the intersection of compliance management and risk management and included the terms in the title, abstract, or keywords; (ii) documents in English; (iii) documents published since 2005. I excluded from the search those studies that used the term compliance outside of an organizational science perspective, such as in a medical sense. The selected documents are presented in Table 6.

Table 6: Documents of the literature review
Source: Benedek, Bognár, 2024

Bibliographic information of the publication	**Country of research**	**Approach/methodology**
Basel Committee on Banking Supervision, 2005	Switzerland	high-level paper on compliance risk and the compliance function in banks
Birindelli, Ferretti, 2008	Italy	questionnaire
Sathye, Islam, 2011	Australia	method of analogy, scorecard of risk assessment based on the literature on credit-scoring models
Birindelli, Ferretti, 2013	Italy	literature review, theoretical model of an efficient internal control system
Esayas, Mahler, 2015	Norway	modeling of compliance risk identification and assessment
Losiewicz-Dniestrzanska, 2015	Poland	literature review and proposal of quantitative indicators in compliance risk monitoring
Nicolas, May, 2017	USA	practical guidance for developing a compliance risk assessment
Naheem, 2019	Germany	literature review and surveys
Achkasova et al. 2021	Ukraine	cognitive modeling method based on the construction of a fuzzy cognitive map

I have collected five explicit definitions of compliance risk from the following organizations/authors: Basel Committee on Banking Supervision (2005), Italian National Bank (2008), Polish Financial Supervision Authority (2011), Nicolas and May (2017), and ISO

37301:2021 standard (2021). The first, second, and last sources share a common element: the sources of compliance requirements can be voluntarily chosen obligations.

While legal risks are externally focused, compliance risks take into account both the internal and external environment and include noncompliance with self-regulatory norms (Esayas, Mahler, 2015). Furthermore, reputational risks, which are excluded from legal and operational risks, are also included in compliance risks. Thus, operational, legal, and compliance risks partially overlap (Birindelli, Ferretti, 2013).

Related to the second research question, I examined what the compliance risk assessment process is according to the literature. According to Nicolas and May (2017), the compliance risk assessment process begins with the identification of the main inherent risks within a business or legal entity. Risk identification examines how a compliance requirement – obligation or prohibition – can lead to risk. Risk identification can be either requirement-based or fact-based (Esayas, Mahler, 2015), and both approaches are equally relevant. In the requirement-based approach, experts aim to identify what triggers the legal norm, such as what actions can lead to violations. In contrast, in the fact-based approach, business processes are assessed to identify potential areas of noncompliance. The advantage of the fact-based approach is that it allows for the reuse of risks previously identified in other areas (Esayas, Mahler, 2015).

According to Łosiewicz-Dniestrzańska (2015), risks can be described by four factors: nature (event or incident), source (persons or units, such as internal control or operational risk reports, whistleblowing), and cause and effect (impact). Measuring risk compliance in banks usually involves creating overly simplified risk matrices that determine the extent of risk (Łosiewicz-Dniestrzańska, 2015, Naheem, 2019). Esayas and Mahler (2015) found that the identification of compliance risks is usually done in unstructured or semi-structured brainstorming sessions, relying on the expertise of legal professionals. Instead, they propose a requirements-driven, five-step process for structured identification and assessment of legal and compliance risks. The graphical modeling they propose can break down complex regulations into easily understandable elements, but there is a risk of information loss during regulatory transformation. The benefits of a structured approach to risk identification include reduced subjectivity. In addition, visualization facilitates communication between experts from different backgrounds.

The purpose of compliance risk assessment is to identify areas of significant risk and where controls are needed to mitigate risks (Nicolas, May, 2017). In the early stages of compliance risk assessment, there was no standard, predefined methodology for assessing compliance risks, and banks used qualitative or mixed methods to calculate risk exposure, such as qualitative assessments based on indicators or self-assessments of the frequency and severity of risk and the effectiveness of controls. (Birindelli, Ferretti, 2008)

Łosiewicz-Dniestrzańska (2015) suggests that the probability and impact of a risk be determined independently on a scale from 1 to 5, and that the overall risk be calculated as the product of impact x probability. The numerical values (1-25) can then be converted into a 5-point risk rating (mild, moderate, significant, severe, catastrophic). In practice, the accepted scale is often narrower and consists of only three categories (green, yellow, red), where, like on a heat map, yellow indicates a warning and requires corrective action (Łosiewicz-Dniestrzańska, 2015).

Esayas and Mahler (2015) highlight that the risk appetite of individuals performing risk assessments can vary significantly. Therefore, assessments are subjective in the absence of a formalized approach to compliance risk assessment. Historical data can help estimate the likelihood and impact of compliance risks.

Compliance risk assessment forms the basis for implementing compliance management systems and allocating resources to address identified risks. The following control mechanisms can be useful for internal processes: training, segregation of duties, application of the “four eyes” principle, legal opinions, physical security, as well as system mechanisms (access rights, exclusions), supervision and monitoring, and testing (Nicolas, May, 2017, Łosiewicz-Dniestrzańska, 2015).

Quantitative tools for compliance risk monitoring are mainly based on simple, easily accessible indicators, which often overlap with those used by operational risk management. These are based on historical data (e.g., the number of delayed corrective actions, the number of customer complaints submitted to regulatory authorities, the rate of completion of training, and the number and frequency of detected violations) (Łosiewicz-Dniestrzańska, 2015; Asenov, 2015). It is important to note that indicators do not measure risk, but they are valuable in illustrating trends and can be early warning tools.

In addition to academic sources, I examined what additional insights organizational development and business consulting firms have published in reports and articles. According to KPMG experts, the development of technology and automation offers enormous opportunities for increasing efficiency, as data analysis solutions help identify outliers, prevent, detect, and address potential violations, and make evidence-based decisions. (Matsuo, Staines, 2020)

According to an Ernst & Young report (EY, 2021), emerging technologies can improve early detection of risks (e.g., use of artificial intelligence in fraud detection, continuous monitoring instead of sampling), contribute to less reliance on manual processes, and improve risk assessment processes. To address identified and assessed risks, EY recommends four strategies: risk avoidance, risk transfer (to a third party), risk mitigation (reducing the likelihood), and risk acceptance (controlling and monitoring expected risks). (EY, 2021)

Deloitte published a report on compliance risk assessment in 2015. (Deloitte, 2015) The methodology distinguishes between the legal, financial, business, and reputational impacts of inherent risks. Key practical recommendations include collecting data across functions, building on existing content (e.g., reports) and methodology, clear risk ownership for transparency, and producing actionable and practical risk assessments (priorities, action plans, monitoring). Other recommendations include using plain language and iterating on risk assessments regularly. (Deloitte, 2015)

The answers to the research questions are presented below. What are the meanings of the term compliance risk? The definitions collected mainly reflect the causes and effects of compliance risks. The definition from the Basel Committee (2005) is widely accepted as a reference. This definition consists of a cause and an effect part. The cause for noncompliance can be "noncompliance with laws, regulations, rules, related self-regulatory organization standards”. The impact is divided into three areas: legal sanctions, financial loss, and reputational damage.

On the side of compliance sources, market standards and voluntarily chosen requirements can be added to the Basel definition. However, the impact side is significantly different in the definition of the ISO 37301:2021 standard. Although the consequences are not divided into three areas, the probability of occurrence is an essential part of the definition of the standard. Therefore, in the article, I proposed a new definition of compliance risk.

According to the new definition, *compliance risk refers to an event with the likelihood of potential regulatory, financial, or reputational losses for the organization due to noncompliance with regulations or voluntary obligations*.

About the second research question, I examined the compliance risk assessment process according to the literature. I present five findings in this regard.

1) The literature is not uniform, even about compliance risk management activities (the interpretation, content of risk reduction, control, and monitoring activities, and their relationship are not uniform). Few specific methods and techniques have been developed for identifying and modeling compliance risks. Scientific and business reports rarely cite the current ISO standard relevant to the topic. Therefore, it is advisable to apply general risk assessment approaches and methodology to the specific compliance risk area.
2) Several publications see value in close cooperation between operational risk management and compliance management. Collaboration with other elements of internal control, such as operational risk management and internal audit, can reduce compliance costs.
3) The severity of the risk impact should be assessed independently of the analysis of controls. Organizations need help quantifying the practical effects of risks. The proper use of historical data is necessary, but not sufficient, as it can be incomplete or misleading (Birindelli, Ferretti, 2008)
4) Partial risks may remain hidden if organizations only use the traditional risk matrix (probability vs. impact) (Bognár, Benedek, 2021a, Bognár, Benedek, 2021b). The partial risk map methodology provides a more efficient and detailed picture of the risk assessment results.
5) Individual risk assessment is strongly underrepresented in the literature compared to group assessment. The study by Esayas and Mahler (2015) suggests that the visualization of risk assessment and the establishment of cross-functional teams compensate for the difficulties of individual, professional, and verbal interpretation of risks. Visual representation of risks can facilitate shared understanding and clearer communication on compliance issues.

Based on the literature review and the above findings, I propose the following structured compliance risk assessment process. As a starting point for the process, compliance obligations provide input to the compliance risk assessment process, which consists of three main steps (Figure 5):
1) identification of compliance risks,
2) compliance risk analysis (analysis of noncompliance, its likelihood and impact, and assessment of detectability by current controls),
3) compliance risk assessment (prioritization of risks).

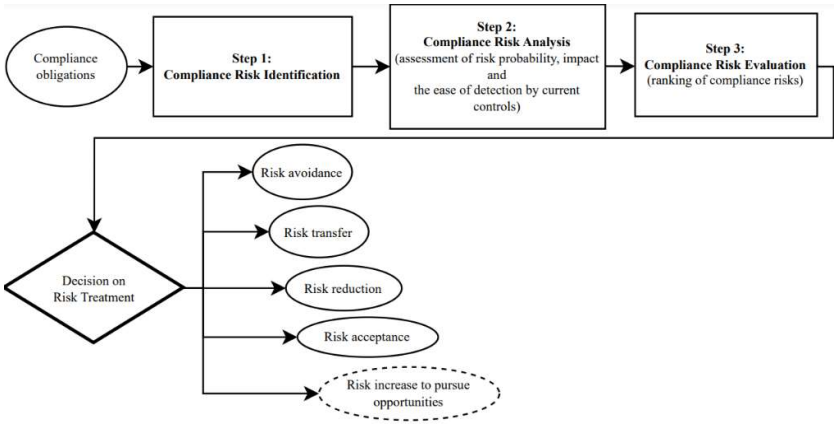


Figure 5: Structured compliance risk assessment process
Source: Benedek, Bognár, 2024, p. 257

The structured compliance risk assessment process ends with a decision. The five possible outcomes of the decision are: the organization avoids, accepts, transfers, reduces the risk, or increases it to exploit business opportunities. This structured approach can reduce subjectivity in making compliance decisions and resource allocation. Better results can be achieved with a structured approach than during unstructured brainstorming.

About the third research question, I examined what gaps and potential research directions can be identified based on the literature. I will not detail the answer to this question here, but will present it later, among future research directions.

Contribution of the sub-chapter to the habilitation theses:

- I have created a new definition of compliance risk based on a combination of several previous definitions.
- Compliance risk assessment can be improved by applying structured frameworks and methodologies. To this end, I have developed a new compliance risk assessment process (Figure 5).
- It has been confirmed that the analysis of controls is a significant part of the risk assessment, since detectability is an essential part of the risk. I assign this point to thesis T1.
- I assign the entire article to these T4 and T5.

Future research and application possibilities

The presented habilitation theses are related to four selected articles. My further related works also have an impact on future research. I see two main research directions. In one direction, the development of risk assessment methods continues. In the other direction, I intend to explore and analyze the connection points between quality management and compliance, using both theoretical and empirical approaches.

Possible future research directions:

- Examination of individual and group expert risk assessments, further development of the PRISM methodology. Integrating PRISM with BWM or fuzzy logic and its application to the evaluation of compliance risks.
- Including case studies with a larger sample size using existing methods, and thus formulating more nuanced conclusions. I can imagine research where the regional impact in risk assessment can be described based on regional categorization variables found in a bank's domestic and international branch network.
- The evaluation of the effectiveness of compliance risk reduction is still in its infancy, both theoretically and practically. A possible research direction is to measure the impact of different compliance risk management strategies and develop a theoretical model for this.
- Empirical research that examines the integration of compliance risk assessments with other types of risk assessments (such as operational risks).
- Developing a compliance maturity model based on excellence models and examining its applicability.
- The developed compliance QFD method focuses on institutional-level quality in higher education, and does not aim at analyzing and developing quality at the program or course level. Here, I see the possibility of further development towards other quality levels.
- Compliance QFD primarily reflects the expectations of students among the stakeholders. The process can be developed by involving multiple stakeholders. Furthermore, the compliance QFD process can be tested in other sectors beyond higher education.

Resources

Alshare, K.A., Lane, P.L., Lane, M.R. (2018). "Information security policy compliance: a higher education case study", Information and Computer Security, Vol. 26 No. 1, pp. 91-108. https://doi.org/10.1108/ICS-09-2016-0073

Asenov, E. (2015). Characteristics of Compliance Risk in Banking. Economic Alternatives, 2015, 4, 20-28. https://www.unwe.bg/uploads/Alternatives/2-Asenov.pdf

Ashton, J. (2015), "15 years of whistleblowing protection under the Public Interest Disclosure Act 1998: are we still shooting the messenger", Industrial Law Journal, Vol. 44 No. 1, pp.29-52. https://doi.org/10.1093/indlaw/dwu029

Achkasova, S.; Bezrodna, O.; Ohorodnia, Y.: Identifying the volatility of compliance risks for the pension custodian banks. Banks and Bank Systems, 2021, 16(3), 113-129. https://doi.org/10.21511/bbs.16(3).2021.11

AIRMIC (2010). A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000, AIRMIC, London, UK

Bamber, C. (2022). "The Role of Enterprise-wide Risk Assessment in Developing Resilient Higher Education Institutions", Sengupta, E., Blessinger, P. and Nezaami, N. (Ed.) Governance and Management in Higher Education (Innovations in Higher Education Teaching and Learning, Vol. 43), Emerald Publishing Limited, Bingley, pp. 13-33. https://doi.org/10.1108/S2055-364120220000043002

Basel Committee on Banking Supervision. 2013. Principles for Effective Risk Data Aggeration and Risk Reporting. Available online: http://www.bis.org/publ/bcbs222.pdf (accessed on 6 September 2021).

Becket, N., Brookes, M. (2008). "Quality management practice in higher education – What quality are we actually enhancing?", Journal of Hospitality, Leisure, Sport and Tourism Education, Vol. 7 No. 1, pp. 40-54. https://doi.org/10.3794/johlste.71.174

Bederna, Zs., Rajnai, Z., Szadeczky, T. (2021). "Further Strategy Analysis of Cybersecurity Incidents", Land Forces Academy Review, Vol. 26 No. 3, pp.251-260. https://doi.org/10.2478/raft-2021-0032

Benedek, P., Surman, V. (2025). Compliance QFD – how compliance contributes to quality in higher education. Educational Research and Evaluation, 30(5–6), 345–368. https://doi.org/10.1080/13803611.2024.2437425

Benedek, P., Bognár, F. (2024). Compliance Risk Assessment - Results of a Comprehensive Literature Review. Acta Polytechnica Hungarica 21(6), 243-262. https://doi.org/10.12700/APH.21.6.2024.6.13

Bernardi, R.A., Landry, A.C., Landry, E.E., Buonafede, M.R., Berardi, M.E. (2016). "What actions can be taken to increase whistle-blowing in the classroom?", Accounting Education, Vol. 25 No. 1, pp.88-106. DOI:10.1080/09639284.2015.1107496

Birindelli, G.; Ferretti, P. (2008). Compliance risk in Italian banks: the results of a survey, Journal of Financial Regulation and Compliance, 2008, 16, 4, pp. 335-351. https://doi.org/10.1108/13581980810918404

Birindelli, G., Ferretti, P. (2013). Compliance function in Italian banks: organizational issues, Journal of Financial Regulation and Compliance, 2013, 21, 3, pp. 217-240. https://doi.org/10.1108/JFRC-07-2012-0027

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

Bognár, F., Benedek, P. (2021b). A Novel Risk Assessment Methodology – A Case Study of the PRISM Methodology in a Compliance Management Sensitive Sector. Acta Polytechnica Hungarica, 18(17), pp. 89-108.

Bognár, F., Böcskei, E. (2022). Potential model to support the achievement of corporate carbon neutrality. Public Finance Quarterly, 67(3). https://doi.org/10.35551/PFQ_2022_3_4.
Bognár, F., Hegedűs, Cs. (2022). Analysis and Consequences on some Aggregation Functions of PRISM (Partial Risk Map) Risk Assessment Method. Mathematics, 10(5), 676.
Bognár, F., Szentes, B., Benedek, P. (2023). Compliance Risk Assessment in the Banking Sector – Application of a Novel Pairwise Comparison-based PRISM Method. Complexity, Paper: 9165815, https://doi.org/10.1155/2023/9165815
Bugdol, M., Jedynak, P. (2022), "Quality objectives in management systems – their attributes, establishment and motivational function", International Journal of Quality & Reliability Management, Vol. 39 No. 1, pp.115-136. https://doi.org/10.1108/IJQRM-05-2020-0173
Choi, S, Chun, YH. (2021). "Accountability and organisational performance in the publicsector: Analysis of higher education institutions in Korea", Public Admin. 2021;99: pp.353–370. https://doi.org/10.1111/padm.12683
Dawson, J. R. (2009). "Audit and Compliance – A Natural Partnership", College & University Auditor, Vol. 52 No. 3, pp.4.
Deloitte (2015). Compliance risk assessments, The third ingredient in a world-class ethics and compliance program, Deloitte, 2015. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-compliance%20riskassessments-02192015.pdf
Do, Q. T. N., Pham, H. T., Nguyen, K. D. (2017). "Chapter 12 - Quality Assurance in the Vietnamese Higher Education: A Top-Down Approach and Compliance-Driven QA", Shah, M., Do, Q. T. N. (Ed.), The Rise of Quality Assurance in Asian Higher Education, Chandos Publishing, Hull, pp.191-207. https://doi.org/10.1016/B978-0-08-100553-8.00005-7
Dorasamy N. (2013). "Good Governance and Whistleblowing: A Case of a Higher Education Institution (HEI) in South Africa", Journal of Social Sciences, 34:2, pp. 105-114. https://doi.org/10.1080/09718923.2013.11893122
Eckert, C., Gatzert, N. (2019). 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.
Esayas, S., Mahler, T. (2015). Modelling compliance risk: a structured approach. Artif. Intell. Law, 2015, 23, 3 (September 2015), 271–300. https://doi.org/10.1007/s10506-015-9174-x
EY (2021). Reshaping the future of compliance with emerging technologies, Ernst and Young, 2021. https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/news/2021/07/ey-forensics-survey-reshaping-the-future-of-compliance-with-emerging-technologies.pdf
Hatta, N.N.M., Abdullah, S.N.H.S., Miskon, S. (2019). "Social Media facilitate Compliance Communication in Higher Education Institutions", 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), pp.1-6. https://doi.org/10.1109/ICRIIS48246.2019.9073676
Hina, S., Selvam, D.D.D.P., Lowry, P. B. (2019). "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world", Computers & Security, Vol. 87, 101594, https://doi.org/10.1016/j.cose.2019.101594
Hwarng, H. B., Teo, C. (2001). Translating customers' voices into operations requirements - A QFD application in higher education. International Journal of Quality & Reliability Management, 18 (2), 195–226. https://doi.org/10.1108/02656710110379075
IIA (2013). The Three Lines of Defense in Effective Risk Management and Control. https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf letöltés: 2025/08/05

IIA. (2019). The IIA's Three Lines Model. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf
ISO (2014). Compliance Management Systems Guidelines. ISO 19600:2014., ISO, Geneva
ISO (2021). "Compliance management systems - Requirements with guidance for use. ISO 37301:2021", ISO, Geneva
Jackson, N. (1997). "Academic regulation in UK higher education: part I - the concept of collaborative regulation", Quality Assurance in Education, Vol. 5 No. 3, pp. 120-135. https://doi.org/10.1108/09684889710174459
Liu, H., Liu, L., Liu, N. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. Expert Systems with Applications 40: 828–38. https://doi.org/10.1016/j.eswa.2012.08.010.
Lipton M., Neff, D.A., Brownstein, A.R., Rosenblum, S.A., Savarese, J.F., Emmerich, A.O., Silk, D.M., Carlin, W.M., Savitt, W.D., Anders, D.B., Wahlquist, A.K., Cain, K.L., Eddy, S.K., Niles, S.V., McLeod, R.A., Reddy, A., Adlerstein, D.M., Lu, C.X.W., Munshi, R.I., Westphal, C. (2022). "Risk Management and the Board of Directors", https://www.wlrk.com/webdocs/wlrknew/ClientMemos/WLRK/WLRK.28180.22.pdf letöltés: 2025/08/06
Losiewicz-Dniestrzanska, E. (2015). Monitoring of Compliance Risk in the Bank. Procedia Economics and Finance, 26, 800-805.
Matsuo, A., Staines, K. (2020). Effective compliance programs – Updated DOJ guidance, KPMG Regulatory Alert,. https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/effective-compliance-programs.pdf
Miguel, P.A.C. (2005). "Evidence of QFD best practices for product development: a multiple case study", International Journal of Quality & Reliability Management, Vol. 22 No. 1, pp.72-82. https://doi.org/10.1108/02656710510573002
Nagy, S., Somosi, M. (2020). "Students' Perceptions of Sustainable Universities in Hungary: An Importance-Performance Analysis", Amfiteatru Economic, 22(54), pp. 496-515.
Naheem, M. A. (2019). Anti-money laundering/trade-based money laundering risk assessment strategies – action or re-action focused?, Journal of Money Laundering Control, 2019, 22, 4, pp. 721-733. https://doi.org/10.1108/JMLC-01-2016-0006
Nicolas, S., May, P. V. (2017). Building an effective compliance risk assessment programme for a financial institution. Journal of Securities Operations & Custody, 2017, 9(3), pp. 215-224.
Noda, A., Hou, A.Y.C., Shibui, S., Chou, H.C. (2018). "Restructuring quality assurance frameworks: A comparative study between NIAD-QE in Japan and HEEACT in Taiwan", Higher Education Evaluation and Development, Vol. 12 No. 1, pp.2-18. https://doi.org/10.1108/HEED-12-2017-0008
Olt, P. A. (2020). "The implicit costs of regulatory compliance in higher education: A case study", Journal of Higher Education Management, Vol. 35 No. 2, pp.28-43.
Romzek, B. S., Dubnick, M. J. (1987). 'Accountability in the Public Sector: Lessons from the Challenger Tragedy', Public Administration Review 47: 227–238.
Root Martinez, V. (2019). "The Compliance Process", 94 Indiana Law Journal, pp. 203-251.
Sahney, S., Banwet, D.K., Karunes, S. (2010). "Quality framework in education through application of interpretive structural modeling: An administrative staff perspective in the Indian context", The TQM Journal, Vol. 22 No. 1, pp.56-71. https://doi.org/10.1108/17542731011009621

Salvioni, D. M., Gennari, F., Bosetti, L. (2016). 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

Sathye, M., Islam, J. (2011). Adopting a risk-based approach to AMLCTF compliance: the Australian case, Journal of Financial Crime, 2011, 18, 2, pp. 169-182. https://doi.org/10.1108/13590791111127741

Surman, V., Tóth, Zs.E. (2021). "Service Quality Measurement in Higher Education", Proceedings of FEB Zagreb 12th International Odyssey Conference on Economics and Business, Croatia, Sibenik, pp.556-570.

Surman, V. (2021). "Service quality measurement and evaluation in higher education – The improvement of a service quality framework for project work-type courses", Doctoral Dissertation https://repozitorium.omikk.bme.hu/items/8b2b0111-bb75-4bbe-9dd3-e38526c3eb50 letöltés: 2025/08/07

Surman, V., Tóth, Zs.E., Danó, Gy. (2022). "Defining service quality attributes at different levels of operation in higher education institutions: How could the service quality perceptions of students contribute to a better understanding of improvement directions?", Proceedings of FEB Zagreb 13th International Odyssey Conference on Economics and Business, Croatia, Dubrovnik, pp.916-927.

Vezzetti, E., Marcolin, F., Guerra, A.L. (2016). "QFD 3D: a new C-shaped matrix diagram quality approach", International Journal of Quality & Reliability Management, Vol. 33 No. 2, pp.178-196. https://doi.org/10.1108/IJQRM-07-2013-0112

Yadav, V., Gahlot, P. (2022). "Green Lean Six Sigma sustainability-oriented framework for small and medium enterprises", International Journal of Quality & Reliability Management, Vol. 39 No. 7, pp.1787-1807. https://doi.org/10.1108/IJQRM-08-2021-0297