Compliance Risk Assessment – Results of a Comprehensive Literature Review

Petra Benedek, Ferenc Bognár

Department of Management and Business Economics, Faculty of Economic and Social Sciences, Budapest University of Technology and Economics
Műegyetem rkp 3, H-1111 Budapest, Hungary
benedek.petra@gtk.bme.hu, bognar.ferenc@gtk.bme.hu

Abstract: Today's terminology and definitions of compliance risk are various, and the description of compliance risk assessment is heterogeneous in the literature. These differences result in different expectations, processes, and methodologies in practice, which do not support the widespread adoption of standardized compliance management systems. This study is based on a comprehensive literature review. It aims to redefine compliance risk and propose a structured model for the compliance risk assessment process. The study provides a new framework for compliance risk assessment based on findings and gaps in scientific papers, business reports, and relevant standards. It also introduces the Digital Operational Resilience Act and its compliance aspects.

Keywords: compliance risk; risk assessment; risk identification; DORA; PRISM

1 Introduction

Organizations increasingly realize that they must address the issue of compliance in their operations. New rules and regulations go beyond national borders while increasing in quantity and extent. Regardless of size, sector, and other parameters, organizations are affected by a complex, ever-changing regulatory environment and are subject to enforcement actions, sanctions, fines, and reputational risk.

This paper focuses on the various interpretations of compliance risk and the compliance risk assessment process. In this study, the definitions of compliance risk are collected from the literature to answer the following research questions:

RQ1. What meanings does the term compliance risk contain?

RQ2. What does the compliance risk assessment process look like according to the literature?

RQ3. What are the gaps in the current literature that future research might explore?

In this section, a brief introduction to compliance risks is presented. A frequently referred definition of compliance risk states that it is the organization's exposure to potential legal or regulatory sanctions, financial loss, or a loss of reputation due to the organization's failure to comply with laws and regulations [1]. Compliance risk also includes failure to comply with internal policies or best practices on various topics, like data protection, which could lead to the inability to operate the business.

The term "compliance function" refers to the workgroup which carries out the compliance activities [1]. While the independence of the compliance function is necessary to avoid conflict of interest between compliance and other units, close cooperation with other internal control functions and the business units is indispensable [1].

The ISO 19600:2014 "Compliance management systems guidelines" recognize a risk-based approach to compliance [2]. The ISO 19600:2014 guidelines for compliance management are aligned with the ISO 31000:2018 risk management guidelines [3] as described in previous works [4,5]. The ISO 37301:2021 Compliance management systems standard [6] supersedes the ISO 19600:2014. The standard follows the PDCA logic, where risk identification is part of the Plan phase, compliance risk mitigation by controls and procedures is part of the Do phase, and measurement and monitoring activities are included in the Check phase.

Organizations may follow frameworks and mechanisms to control compliance risk. One critical activity of compliance management is monitoring changes in the regulatory environment to ensure that the organization is well informed and up-to-date on the requirements it is facing and in understanding its level of compliance. Business continuity is closely related to compliance management. Organizations that are prepared and able to remain operational even during disruptive events (e.g., cyberattacks) instill confidence in their partners and can expect better cooperation.

Ultimately, the board (the governing body) is responsible for reviewing all aspects of an organization's compliance risk, and senior management is responsible for effectively communicating and managing the risks [1]. Compliance risk consists primarily of penalties and other consequences for regulatory noncompliance and reputational risk. The first includes illegal practices, like fraud, theft, bribery, money laundering, and embezzlement. Violation of data protection laws, pollution, environmental damage, and occupational health and safety violations are also common compliance risks. Cloud computing delivers new compliance risks since cloud services might store sensitive or protected data.

It is necessary, to clarify a few other risks that are close or even partially overlap with compliance risks.

1) Reputational risk is a loss in an organization's perceived trustworthiness or integrity. It has a negative impact, resulting in direct losses in revenue, indirect losses of customers, orders, employees, foregone business opportunities, or perception of the brands. Reputational loss is usually a

consequence of another business risk; negative news spreads quickly and beyond the company's control.

2) Integrity risks are current or future threats to an organization's reputation, capital, or results due to inadequate compliance with applicable laws. Integrity risks are partly the risk of insufficient compliance with the law and, on the other hand, the risk of employees engaging in actions that could seriously damage trust in the organization. Examples of integrity risks are money laundering, corruption, and conflicts of interest between staff and clients.
3) Conduct risk refers to the potential inappropriate, unethical, or harmful behavior (such as misleading advertising, insider trading, market manipulation) that could negatively affect customers, investors, and the market. Conduct risk can have serious consequences, damage the institution's reputation, lead to legal and regulatory sanctions, and cause financial losses to customers or investors. Nicolas and May defined conduct risk as any activity or inaction by an organization's personnel that could lead to unfair outcomes for its clients, affect the integrity of the markets, or otherwise jeopardize the organization's reputation or financial situation [7].

The Digital Operational Resilience Act (DORA) is a legislative proposal of the European Commission which aims to increase the operational resilience of the EU financial sector by creating a harmonized framework for digital operational resilience. The proposal aims to ensure financial institutions can withstand and respond to various operational risks, including cyberthreats, IT disruptions, and other technology-related risks. According to present plans, it shall apply from January 2025 [8]. DORA compliance is a current challenge for thousands of financial entities and ICT service providers operating within the EU and the ICT infrastructure supporting them from outside the EU.

The importance of DORA lies in the financial sector increasingly relying on digital technology, which presents new risks and challenges regarding operational flexibility [9]. Cyberattacks, IT failures, and other technology-related incidents can cause significant disruption to financial institutions and have far-reaching consequences for the financial system and the economy. DORA is expected to significantly impact financial institutions operating in the EU, as they must meet new requirements and standards for digital operational flexibility. This includes establishing and maintaining effective governance and risk management arrangements, conducting regular testing and exercises to assess operational resilience, and reporting significant events to the relevant authorities.

The financial sector witnesses a change in the regulatory perspective from defense and protection to building resistance, resilience, and flexibility [10]. Therefore, an Information and Communication Technology (ICT) risk management framework to manage ICT risks is strongly connected to compliance risk management since some risks may have regulatory, reputational, or both effects.

This paper is organized as follows. Section 2 introduces the methodology, while Section 3 presents the results. In Section 4, the results are discussed, highlighting managerial implications.

2 Methodology

This research is based on a comprehensive literature review. The data extraction process was designed based on the research questions to highlight the similarities and differences among the results of the studies.

For this study, the authors used the Scopus digital database, which many research studies have used, to select and identify the most relevant studies. The selection process was guided by specific keywords included in the following search: compliance risk OR compliance assessment OR compliance risk evaluation. The search was conducted in July 2023 following the logic of the PRISMA 2020 statement.

The search was extended to one regulatory documents outside the Scopus [1], that was used as references in the first set of research studies. Additionally, reports and white papers published by consultancy firms are reviewed in Section 3.3.

The following inclusion criteria have been defined for examining the research questions: (i) journal papers and regulatory reports that dealt with 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. In addition, papers using the term outside of an organizational perspective (e.g., medical use) were excluded from the research. The selected documents are presented in Table 1.

Table 1
Documents of the literature review

Bibliographic information of the publication	**Country of research**	**Approach/methodology**
Basel Committee on Banking Supervision, 2005 [1]	Switzerland	high-level paper on compliance risk and the compliance function in banks
Birindelli, Ferretti, 2008 [12]	Italy	questionnaire
Sathye, Islam, 2011 [13]	Australia	method of analogy, scorecard of risk assessment based on the literature on credit-scoring models
Birindelli, Ferretti, 2013 [14]	Italy	literature review, theoretical model of an efficient internal control system
Esayas, Mahler, 2015 [15]	Norway	modeling of compliance risk identification and assessment

Losiewicz-Dniestrzanska, 2015 [11]	Poland	literature review and proposal of quantitative indicators in compliance risk monitoring
Nicolas, May, 2017 [7]	USA	practical guidance for developing a compliance risk assessment
Naheem, 2019 [16]	Germany	literature review and surveys
Achkasova et al. 2021 [17]	Ukraine	cognitive modeling method based on the construction of a fuzzy cognitive map

3 Results

The results are presented along with the research questions. Section 3.1 reflects on the definitions of compliance risks and the boundaries of compliance risk management. Section 3.2 provides a detailed insight into the risk assessment process. Finally, Section 3.3 delivers additional information from the business reports and surveys.

3.1 Definitions and Insights on Compliance Risk

The following explicit definition of compliance risk has been collected:

1) The definition of compliance risk is given by the [1] as follows: “The expression "compliance risk" is defined in this paper as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, "compliance laws, rules, and standards").” This definition is widely accepted and used [11, 14].
2) The Bank of Italy provides another definition. "The risk of non-compliance with rules is the risk to incur in judicial or administrative sanctions, material financial losses or loss of reputation as a result of infringement of mandatory rules (laws and regulations) or of self-regulation (that is statutes, codes of conduct, codes of self-discipline)" [12].
3) The Polish Financial Supervisory Commission defined noncompliance risk "as a result of a bank's failure to comply with legal requirements and recommendations set out by the Polish Bank Association" [11].
4) Nicolas and May [7] define compliance risk as the risk of legal or regulatory sanctions or financial loss resulting from failure to comply with applicable laws, regulations, rules, and related market standards.
5) The ISO 37301:2021 standards define compliance risk as likelihood of occurrence and the consequences of not fulfilling the organization’s (mandatory or voluntarily chosen) compliance obligations [6].

While legal risks have an external focus, compliance risks focus on the internal and external environment and include failures to comply with self-regulatory standards [15]. Furthermore, reputational risks that are excluded from legal and operational risks are also included in compliance risks. There is a partial overlapping of operational, legal, and compliance risks [14].

Requirements for the efficient and effective management of compliance risks include (1) establishing an independent function and (2) the definition of the person responsible for compliance risk management [12]. The independence of the compliance function, its formalization of responsibilities, and relationship with other control functions are general requirements [14].

In principle, the compliance function and the internal audit function should be separated to ensure that the activities of the compliance function are subject to an independent review [1]. While compliance risk assessment is primarily the responsibility of the compliance functions, a review (control) responsibility lies within the internal audit, and supervision is the governing body's responsibility [1]. In contrast, [7] emphasized that the business should own the compliance risk assessment process, and the compliance function should only assist in its planning and execution.

With internal audit, some synergies are related to risk and control assessment methods, risk mapping, and promoting a strong "control culture" [12]. Unlike the top-down approach of internal audit, compliance management is a bottom-up activity with an analytical vision of compliance risks and the processes involved [14].

Operational risks, legal risks, and compliance risks often overlap. Cross-cases emerge from a "grey zone" that includes breach of contract (classified as an operational risk event) and the bank's liability for improper conduct leading to legal risk lawsuits [14]. Although the European Network and Information Security Agency [18] have published recommendations on cloud computing risk assessment, there are no specific guidelines for identifying legal risks.

Both compliance and operational risk management are second-level control structures whose task is to identify the risks inherent in the processes implemented by the various functions [14]. A cooperative or integrated approach to risks can create effective synergies facilitated by shared risk identification, risk indicators, business environment analysis, and information exchange and validation [14]. Consultations with business units (e.g., internal audit, operational risk unit, legal or security department) and using the results of their audits and information from their reports can contribute to better compliance monitoring [11].

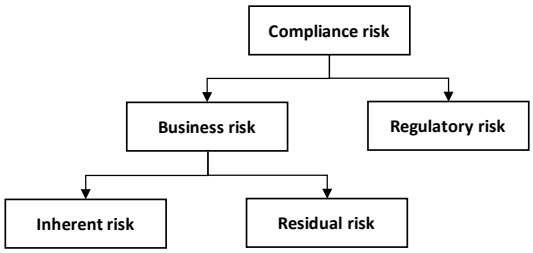

Figure 1
The grouping of compliance risks, own editing based on [13 p. 176.]

Compliance risks can be grouped under two categories: regulatory risk and business risk (Figure 1). Regulatory risks come into being because of the inability to comply with legislation requirements. Australia's financial intelligence unit divides business risk into inherent and residual risk. Inherent risks are identified and managed and come from various sources like customers (i.e., politically exposed people, customer complaints), products or services, and previous compliance reports [7, 13]. Inherent risks are identified, controls to mitigate the risks are listed, and the resulting residual risk calculations are classified in terms of potential financial, regulatory, and public reputational damage to the entity [7]. Methods for identifying inherent risk should include quantifying control effectiveness [7]. The basic idea behind quantifying inherent business risks is to pre-identify key factors and combine or weight them into a quantitative score, which can be directly interpreted as the probability or used as a classification system. Residual risk is the risk left, despite a robust risk management system [13].

3.2 The Compliance Risk Assessment Process

Compliance risk management is a systematic process for identifying, analyzing, and prioritizing an organization's compliance risks. According to Nicolas and May [7], the compliance risk assessment process starts with identifying the main inherent risks within a business or legal entity. In this section, the next steps are risk analysis and evaluation, followed by risk treatment.

3.2.1 Risk Identification

Risk identification examines how a compliance requirement—obligation or prohibition—may lead to risk. Risk identification can be requirements-centered or facts-centered [15], and both approaches are equally relevant. In the requirements-centered approach, experts aim to identify what might trigger the legal norm through guiding questions like what actions could lead to violations.

In contrast, business processes are evaluated in the facts-centered approach to identify potential noncompliance areas. The benefit of a facts-centered approach is that it is possible to reuse previously identified risks from other areas and assess their compliance implications [15].

Nicolas and May [7] recommend combining the above approaches as follows:

1) The regulatory requirements are the starting point.
2) The risk inventory is prepared based on them.
3) The next step is the detailed examination of the risks through the relevant business processes and identifying (yet not assessing) relevant actual controls.

Risk identification builds on the collection of timely and accurate data (even independent third-party data) and on identifying the relevant legal obligations by establishing an applicable legal framework and evaluating the relevance and importance of specific regulations in the organization's business activities. Risk identification is a critical step for the effectiveness of the subsequent stages of the risk management process [11].

According to Łosiewicz-Dniestrzańska [11], risks can be described by four factors: nature (event or incident), source (people or units, like internal audit or operational risk reports, whistleblowing), cause and effect (impact). Measuring risk compliance in banks usually means creating overly simplistic risk matrices determining the risk degree [11, 16].

Esayas and Mahler [15] found that compliance risk identification is usually made in unstructured or semi-structured brainstorming sessions, relying on lawyers' expertise. Instead, they propose a requirements-centered five-step process for the structured identification and assessment of legal and compliance risks:

1) step: identify the source of the requirements
2) step: list of obligations and prohibitions
3) step: structuring a requirements template
4) step: template-based modeling
5) step: instantiation

"We don't talk the same language when we discuss risks" [15]. Esayas and Mahler highlight the importance of language and possible difficulties in communication as experts from different fields use their vocabularies (e.g., IT, legal). The proposed graphical modeling can break down complex regulations into easily understandable elements. Using templates in the risk identification and assessment steps facilitates modeling and monitoring, while it has the risk of missing information while transforming the regulations. One participant in their case study indicated that risk identification is less challenging than risk assessment.

The benefits of a structured approach to risk identification reduce the subjectivity of compliance decisions. In addition, visualization provides focus and facilitates communication between experts from different backgrounds. Furthermore, the structured approach produces reusable results, so the costs of using the approach can be lower in the long-term [15].

3.2.2 Risk Analysis and Evaluation

Compliance risk assessment is a systematic process for identifying, analyzing, and prioritizing an organization's compliance risks. Compliance risk assessment aims to identify areas of significant risk and where controls are required to reduce risks [7]. The Basel Committee [1] proposes using performance indicators to measure compliance risks. According to the document, compliance risk should be incorporated into the internal audit function's risk assessment methodology, and an audit program should be established that covers the testing of controls proportional to the level of perceived risk. Birindelli [12] suggests defining risk models and Key Performance Indicators as part of the boundary setting of the different management areas. Meanwhile, some risks are simultaneously part of operational and compliance risks (i.e. contract breeches).

By the Second Pillar of Basel 2, it is necessary to quantitatively measure compliance risk in banks [12]. In the early stages of risk assessment, there was no general, predefined methodology for assessing compliance risk, and banks used non-statistical methods to calculate risk exposure, such as [12]:

1) Qualitative assessments based on indicators,

2) Self-assessment of the frequency and severity of the risk and the controls. The aim was to calculate the residual risk present after the controls.

Sathye and Islam [13] distinguish the rule-based and risk-based approaches to compliance. The former means establishing the compliance function based on a catalog of regulations. After collecting the legal requirements, they must be evaluated to implement appropriate measures to ensure compliance. The latter approach means that organizations (reporting entities) can develop compliance procedures and processes and allocate resources appropriately to address the specific risks they face [13, 15]. The benefits of the risk-based approach are the efficient allocation of resources, prioritization of risks, and lesser burdens on customers (and eventually lesser costs). The main steps of the compliance risk management process are risk identification, risk assessment, and developing strategies to manage and mitigate the identified risks [13].

Sathye and Islam [13] propose an inherent business risk assessment scorecard based on credit scoring models. Two risk assessment factors are the risk's likelihood (probability) and impact (severity). For example, they propose a 400-point model that consists of 4 main types of risk for money laundering and terrorism financing, where customers over 300 points would be considered high risk. In general, the outcome of the assessment is, on the one hand, the level of risk identified (high, medium, and low) and, on the other hand, mitigation and control procedures relevant to the risk.

For regulatory risk assessment, Sathye and Islam [13] propose a qualitative self-assessment technique, a questionnaire as a checklist to assess compliance with relevant regulations.

Łosiewicz-Dniestrzańska [11] proposes independently determining risk likelihood and impact on 1-to-5 scales and computing the overall risk as a product of impact x likelihood. Next, we can transform numerical values (1-25) to a 5-scale risk rating (minor, moderate, significant, major, catastrophic). In practice, the accepted scale is often narrower and consists of only three categories (green, amber, red), where, like on a heat map, the amber is a warning and requires corrective measures [11].

Risk assessment is generally carried out in teams, which can be facilitated with software inputs [16]. Teams might include members out of the organization, like customs experts or other third parties. Esayas and Mahler [15] highlight that the risk appetite of the individuals performing the risk assessment might differ significantly. Hence, the evaluations are subjective in case of no formalized approach to compliance risk assessment. Historical data can help simplify the estimation of the probability and impact of compliance risks. In their study, violations have a low, medium, or high-level impact on compliance, depending on the level of remediation (individual, business unit or board, respectively) [15].

According to the 2008 Federal Reserve Supervisory Letter [19], the risk assessment should be based on company-wide standards that define the method and criteria for risk assessment throughout the organization. Also, it should consider the risk inherent in the activity and the strength and effectiveness of the controls designed to mitigate the risk [19]. For assessing risk controls, some questions focus on control design, others on implementation (How reliable is the control? Is it easily bypassed? With control operation: how well does control work in practice?) [7].

Naheem [16] distinguished reactionary versus forward-thinking strategies for anti-money laundering (AML) risk assessment. Reactionary focus means following the the state's agenda and managing development according to regulatory requests. It has the disadvantages of not recognizing risks and other legal challenges, like too fast changes in regulation.

Naheem [16] highlights that improved technology facilitates detecting wrongdoing. Also, this study identified three areas for improvement in detecting and calculating risks: training and experience of the team members and communication with management.

3.2.3 Risk Treatment

The compliance risk assessment forms the basis for implementing compliance management systems and allocating appropriate resources and processes to manage the identified compliance risks. Improvements based on compliance risk assessment lead to better compliance with health and safety and other specific regulations. A compliance risk assessment is a real opportunity to initiate new and update old or unused controls to mitigate risk [7]. Establishing and implementing controls aims to reduce the probability of the causes and their negative consequences. The following control mechanisms can be helpful to internal procedures: training, segregation of duties, application of the "four eyes" principle, legal opinions,

physical security, and system mechanisms (access rights, exclusions), surveillance and monitoring, and testing [7, 11].

Quantitative tools for compliance risk monitoring are mainly based on simple, readily available indicators, often overlapping with those used by operational risk management. They are based on historical data (e.g., the number of overdue corrective action, the number of customer complaints to regulators, ratio of completion of training, and the number and frequency of detected violations) [11, 20, 21]. Please note that indicators do not measure the risk but are valuable in showing the trends and can signal early warnings.

Given the importance of issues related to compliance risk assessment, it is necessary to develop a theoretical basis and tools to assess the potential growth and realization of compliance risks [17].

3.3 The Business Perspective

Traditionally, compliance has been seen as the responsibility of specific business units or functions (i.e., financial regulation, safety and environmental laws, employment standards). Many businesses used a silo approach to compliance and isolated efforts without aligned intent [22].

According to a KPMG survey in 2006, compliance verifies the consistency of internal and bank regulations and advises on legal risk issues, while the risk management function monitors all risks [14]. KPMG emphasizes the importance of compliance risk assessment in developing effective compliance programs. The report highlights key steps in a compliance risk assessment and provides practical advice for organizations to conduct compliance risk assessments [23]. Advancements in technology and automation present tremendous opportunities to innovate and increase efficiency, as data analytics solutions help to identify alerting data, prevent, detect, and respond to potential violations and make evidence-based decisions. Key risk and performance indicators often predict events that can increase an organization's risk exposure and work as alerting signs of potential problems so they can be monitored and mitigated. KPIs and KRIs enable compliance managers to make better decisions and manage compliance risks more effectively. KPMG also presents a maturity model for the integration of data analytics into compliance management [24].

PwC provides practical guidance on compliance risk assessments, including using risk matrices [25]. Compliance testing should be designed around and focused on the organization's most serious threats and aligned with risk appetite and business risk assessment. Mitigation should respond to test results; the most significant identified risks or weaknesses are subject to increased testing. The compliance function typically performs this type of assessment with data from business areas [26].

Boards must provide tangible evidence that they are effectively managing their compliance risks [27]. According to a recent Ernst & Young report [28], emerging technology could improve the early detection of risks (e.g., using AI in fraud detection, continuous monitoring instead of sampling), contribute to less reliance on manual processes, and enhance risk assessment processes. To manage identified and assessed risks, EY proposes four strategies: risk avoidance, risk transfer (to a third party), risk mitigation (reducing the probability), and risk acceptance (controlling and monitoring expected risks) [28].

Another 2021 Ernst & Young study covered 21 European banks, most implementing compliance functions using traditional compliance risk monitoring models. However, there is much interest in adopting technologically advanced models [29].

Deloitte has issued a report on compliance risk assessment in 2015 [30]. In the methodology, they distinguish the legal, financial, business, and reputational impact of inherent risks. The main practical recommendations are data collection from cross-functional specialists, building on existing content (like reports) and methodology, clear risk ownership for transparency, and delivering useable and actionable risk evaluations (priorities, action plans, monitoring). Further recommendations are using simple language and regularly repeating the risk assessment [30].

Deloitte has also developed a Systematic Integrity Risk Analysis (SIRA) methodology that covers all relevant integrity risks and meets the risk assessment requirements outlined in the 4th Anti-Money Laundering Directive. The main steps of the risk analysis are to determine inherent risk, identify controls, determine managed risk, and define mitigating measures [31]. The SIRA methodology also outlines preparation and closing steps after a risk analysis. Deloitte and EY recommend using Robotics Process Automation (RPA) to reduce compliance costs and increase process reliability and regulatory compliance [28, 31].

4 Discussion and Managerial Implications

4.1 Discussion

While the scientific, and business literature generally agree on a risk-based approach to compliance, it is vital to highlight one condition. The risk-based approach works if the regulators empower the businesses and believe they know the risks they face best and should, therefore, be empowered to decide how to identify, mitigate, and manage those risks. In a legal environment, where the regulators think they know the best will go to detailed regulations where a rule-based approach might be more suitable.

One problem with the requirements-centered approach is that regulations are created to respond to crimes (i.e., cybercrime). Following a strictly reactionary strategy to compliance management will expose the organizations to new risks, for example, due to changes in the organization's digital, social, and legal context. Naheem [16] argues for a holistic approach to risk, as organizational failures and fraud often transcend business unit levels and add up across processes. Therefore, the authors propose using a process-based approach to compliance risk management, which could be supplemented with a requirements- or rule-based approach.

The "explain or comply" approach, required by regulatory supervision in some cases, means that organizations that do not comply with laws or codes must explain each noncompliance. Explaining is only valid if it is about meaningful reasoning and not rhetorical misleading by lessening the severity of potential damages or losses in other terms [32].

Bello and Harvey [33] highlight the difficulties of the risk-based approach to anti-money laundering compliance (e.g., confusion on whether the organization's risk perception is in line with the regulator's) and propose the uncertainty-based approach as an alternative. The latter would provide a better understanding of the risk problem within the AML domain and would be more cost-effective while aligning the interests of banks and regulators. The authors of this paper would like to emphasize that AML is a unique field of compliance where the probability assessment of a potential outcome could be even more difficult than in other areas of regulatory compliance.

The answers to the research questions are presented below.

RQ1. What meanings does the term compliance risk contain? The collected definitions mainly reflect on the causes and impact of compliance risks. The Basel Committee [1] definition is widely accepted as a reference. This definition has a cause and an impact part. Causes of noncompliance may be "failure to comply with laws, regulations, rules, related self-regulatory organisation standards." The impact is divided into three areas: legal sanctions, financial loss, and loss of reputation.

On the sources side, market standards [7] and voluntarily chosen requirements [6] could be added to the Basel definition.

However, the impact side is significantly different in the ISO 37301:2021 definition. While the consequences are not divided into three, the likelihood of the occurrence is an essential part of the standard's definition [6].

In this paper, we propose a new definition of compliance risk as follows:

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.

RQ2. What does the compliance risk assessment process look like according to the literature?

1) The literature is not uniform, not even in terms of compliance risk management activities (confusing mitigation, control and monitoring activities and the relation of these). Few specific methods and techniques have been developed to identify and model compliance risks. Scientific and business reports hardly refer to the published ISO guidelines and standards relevant to this topic. Adopting general risk assessment approaches and methodology in the specific compliance risk area would be beneficial.
2) Many publications see value in the close cooperation of operational risk management and compliance management. The information generated in the internal control (internal audit, operational risk management, and compliance management) frameworks can be reused using a structured approach. Cooperation with operational risk management and internal audit can reduce compliance costs.
3) Using mitigation levels as a guideline to estimate the noncompliance impact [15] uses the risk management process backward, creating unreliable risk assessment and inconsistency in the whole process. The severity of risk impact should be assessed independently from the analysis of the controls. Organizations need help to quantify risk impact in practice, and making good use of historical data is necessary but insufficient since it can be incomplete or misleading [12].
4) Nicolas and May [7] highlight that controls are part of the inherent risk. In a sense, actual controls create potential risks. Studies show that partial risks might stay hidden if only the traditional risk matrix (probability vs. impact) is applied [4, 5]. The Partial Risk Map (PRISM) methodology adds the detection factor of failure modes and gives a more efficient and detailed view of the risk assessment results. Root [34] emphasizes that the root causes of compliance violations should be identified.
5) Finally, individual risk assessment, besides group assessment, is highly underrepresented in the literature. Visualization of risk assessment and setting up cross-functional teams in compliance risk identification and assessment is concluded from the study of Esayas [15] to compensate for the difficulties of individual, professional, and verbal interpretations of risks. A visual representation of risks can facilitate a shared understanding and more straightforward communication on compliance issues.

Based on the above inconsistencies of the reviewed literature and the relevant ISO guidelines, the authors propose the following structured compliance risk assessment process.

Among others, compliance obligations provide inputs to the compliance risk assessment process, which has three main steps (Figure 2):

1) compliance risk identification,
2) compliance risk analysis (analysis of probability and impact of noncompliance and assessment of ease of detection by current controls),
3) compliance risk evaluation (ranking of risks).

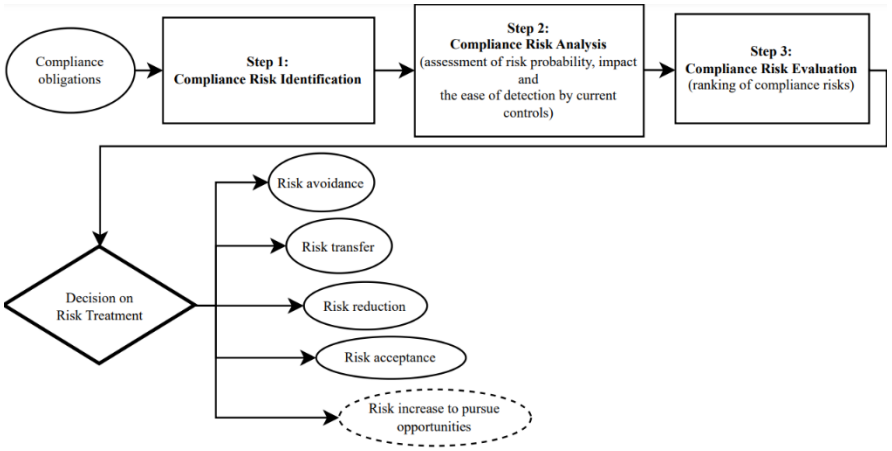

Figure 2
A structured compliance risk assessment process

The structured compliance risk assessment process ends with decision-making. A privacy breach example explains the risk treatment strategies. An organization can avoid the risk of a privacy breach by not using certain technologies. Or an organization may transfer the risk to third parties or external service providers with particular expertise in customer data protection. Alternatively, it can reduce the risk of a privacy breach by investing in measures such as encryption or firewalls. If the organization accepts a certain level of risk, it may plan to respond to incidents by, for example, recovery plans and early detection systems. In some cases, organizations may increase the risk to pursue a business opportunity.

RQ3. What are the gaps in the current literature that future research might explore?

1) Robust methodologies are scarce. Developing robust methods for quantifying compliance risk can improve the accuracy of risk assessment. Future research could propose models for quantifying compliance risk.
2) Research that examines the integration of compliance risk assessments with other types of risk assessments (such as operational risks) can provide a more holistic picture of an organization's risk profile.
3) Data analysis for compliance risk assessment is an emerging field. Future research could explore the intersection of technological innovations with compliance risk assessment.

4) Assessing the effectiveness of compliance risk reduction is still in its infancy. Future studies could develop methodologies to measure the impact of different compliance risk management strategies.
5) Finally, DORA compliance lies in the intersection of information security and compliance management. Future research need to explore what are the compliance aspects of ICT and cyber-risks and how the frameworks can be integrated in theory and practice.

4.2 Managerial Implications

First, similarly to quality management, compliance management was mainly seen as a cost rather than a value-creating function [12]. Nowadays, managing integrity and compliance is critical in creating value and improving reputation.

Transforming legal requirements to risks is a challenge in itself. How can regulations be transformed into threat models and later risks? Darimont and Lemoine [35] propose the KAOS methodology, which transforms regulatory requirements into goals and, after modeling the goals, identifies anti-targets as threats. Also, creating and using templates in risk identification and assessment facilitates communication among experts [15].

Objectivity in assessing consequences can be introduced by creating a structure and criteria for assessing compliance risk. A structured approach can reduce subjectivity in making compliance decisions and resource allocations. Better results can be achieved with a structured approach than an unstructured brainstorming session [15].

When developing a remediation and testing plan, being realistic about what can be accomplished in the given time frame is crucial [7].

As for DORA compliance, Chief Information Security Officers working with DORA can use the ISO/IEC 27001: 2022 standard as a starting point [36]. Compliance with ISO/IEC 27001: 2022 means that an organization has implemented a system to manage risks related to the security of data owned or operated by the company. This standard helps organizations recognize risks and proactively identify and address gaps. An information security management system implemented according to the standard is a tool for risk management, cyber resilience, and operational excellence. ISO 27005: 2022 standard [37] provides a framework and approach to information security and cybersecurity risk management. Most risk management methodologies are derived from this international standard.

The cooperation of compliance and risk management in a coordinated manner, based on shared goals, principles, and values, and having the processes and organizational structures in place to monitor the organization's activities continuously can create value [22].

The Ernst & Young report [28] proposes investment in emerging technologies, investment in the right processes and actions, specialized training and reskill of people, and last but not least, "set the right tone at the top".

Internal audit (responsible for reviewing the effectiveness of the compliance controls) needs to have an in-depth understanding of the various compliance risks to judge the appropriateness of the risk assessment strategy and methodology. Likewise, the board might need training on compliance risks to be able to and be motivated to carry out their responsibility of supervising the compliance risk management of the organization. Root [34] points to the multiplicity of reasons for compliance violations, such as difficulties overseeing compliance programs and the lack of an integrated compliance culture in the corporate structure. Companies starting the "compliance journey" may face resistance from first-line business units [7].

Conclusions

Public or private organizations, regardless of size, sector, and geographic location, are subject to certain regulatory compliance risks. This article has collected various definitions of compliance risk that reflect the prevalence, principles, and scope of compliance management based on a review of nine studies on compliance risk assessment from 2005-2021. The main findings of this research are:

1) A new definition of compliance risk was created based on a combination of several previous definitions.
2) Adopting general risk assessment approaches and methodology tailored to the specific compliance risk area facilitates cooperation with other internal control functions, like operational risk management and internal audit.
3) Analysing controls is a significant part of risk assessment since detectability is an essential part of the risk.
4) Compliance risk assessment can be improved by using structured frameworks and methodology. For this, the authors have developed a structured compliance risk assessment process (Figure 2).

The most important limitation of this study is that some studies on compliance risk assessment may have been excluded from this review due to the inclusion and exclusion criteria developed by the researchers. Future research will focus on quantifying compliance risk to improve the accuracy of risk assessment. Further research could study the use of data analysis in compliance risk assessment. Finally, research needs to explore the compliance aspects of ICT and cyber risks and how the frameworks can be integrated in theory and practice, as necessary for DORA compliance in the future.

References

[1] Compliance and the compliance function in banks, Basel Committee on Banking Supervision, Bank for International Settlements, 2005, https://www.bis.org/publ/bcbs113.pdf

[2] ISO: Compliance management systems - Guidelines, 2014, ISO 19600:2014

[3] ISO: Risk management - Guidelines, 2018, ISO 31000:2018

[4] Bognár F., Benedek P.: A novel risk assessment methodology: a case study of the PRISM methodology in a compliance management sensitive sector. Acta Polytechnica Hungarica, 2021, 18, 7, pp. 89-108, https://doi.org/10.12700/APH.18.7.2021.7.5

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

[6] ISO: Compliance management systems – Requirements with guideance for use, 2021, ISO 37301:2021

[7] Nicolas, S., May, P. V.: Building an effective compliance risk assessment programme for a financial institution. In the Journal of Securities Operations & Custody, 2017, 9, 3, https://www.henrystewartpublications.com/sites/default/files/Nicolas%2C%20Stephanie%20%26%20May%2C%20Paul%20JSOC%209-3.pdf

[8] Regulation (EU) 2022/2554

[9] Grima, S.; Marano, P.: Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings. Risks 2021, 9, 206, https://doi.org/10.3390/risks9110206

[10] Pavlidis, G.: Europe in the digital age: regulating digital finance without suffocating innovation, Law, Innovation and Technology, 2021, 13:2, 464-477, https://doi.org/10.1080/17579961.2021.1977222

[11] Losiewicz-Dniestrzanska, E.: Monitoring of Compliance Risk in the Bank, Procedia Economics and Finance, 2015, 26, pp. 800-805, https://doi.org/10.1016/S2212-5671(15)00846-1

[12] Birindelli, G.; Ferretti, P.: 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

[13] Sathye, M., Islam, J.: 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

[14] Birindelli, G., Ferretti, P.: 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

[15] Esayas, S., Mahler, T.: 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

[16] Naheem, M. A.: 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

[17] 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

[18] ENISA: Cloud computing: benefits, risks and recommendations for information security. In: Catteddu D, Hogben G (eds) European Network and Information Security Agency, 2009

[19] Federal Reserve Supervisory Letter SR 08-08, 16th October, 2008, https://www.federalreserve.gov/boarddocs/srletters/2008/sr0808.htm

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

[21] Compliance in the spotlight, Deloitte LLP, 2013. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-audit-compliance-in-the-spotlight.pdf

[22] Lord, T.; Smith, M.: Compliance + risk management = value, PwC, 2011, https://www.pwc.com/gx/en/oil-gas-energy/publications/pdfs/compliance-plus-risk-management-equals-value.pdf

[23] Matsuo, A.; Staines, K.: Effective compliance programs – Updated DOJ guidance, KPMG Regulatory Alert, 2020, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/effective-compliance-programs.pdf

[24] Gerlach, J., Stryker, N., Matsuo, A., Dookhie, R.: Harnessing data and analytics to transform compliance, KPMG, 2017, https://advisory.kpmg.us/articles/2018/harnessing-data-analytics-to-transform-compliance.html

[25] A practical guide to risk assessment, PricewaterhouseCoopers, 2008, https://web.actuaries.ie/sites/default/files/erm-resources/a_practical_guide_to_risk_assessment.pdf

[26] Franco A., Woolgar, O.: Maximising the benefits from your compliance monitoring programme, PricewaterhouseCoopers, 2022, https://www.pwc.com/jg/en/services/advisory/blogs/maximising-benefits-from-compliance-monitoring-programme.html

[27] Integrity, Compliance & Ethics, Ernst and Young, 2018, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-integrity-compliance-ethics.pdf

[28] 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

[29] Crotaz, S., Lown, J., Niedbala, C.: Compliance transformation: how banks can leverage opportunities now. Ernst & Young, 2021, https://www.ey.com/en_gl/banking-capital-markets-risk-regulatory-transformation/compliance-transformation-how-banks-can-leverage-opportunities-now

[30] 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

[31] Compliance Risk Management Powers Performance, Deloitte, 2018, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-compliance-risk-management-powers-performance.pdf

[32] Shrives, P.; Brennan, N. M.: Explanations for corporate governance non-compliance: A rhetorical analysis, Critical Perspectives on Accounting, 2017, 49, pp. 31-56, https://doi.org/10.1016/j.cpa.2017.08.003

[33] Bello, A. U., Harvey, J.: From a risk-based to an uncertainty-based approach to anti-money laundering compliance. Security Journal, 2017, 30, 24-38, https://doi.org/10.1057/s41284-016-0002-0

[34] Root, V: The Compliance Process, Indiana Law Journal, 2019, 94, 1, Art. 5, https://www.repository.law.indiana.edu/ilj/vol94/iss1/5

[35] Darimont, R.; Lemoine, M.: Goal-oriented analysis of regulations, REMO 2V06: international workshop on regulations modelling and their verification and validation, Luxemburg. 2006, http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-241/paper9.pdf

[36] ISO/IEC: Information security, cybersecurity and privacy protection – Information security management systems, Requirements, 2022, ISO/IEC 27001:2022

[37] ISO/IEC: Information security, cybersecurity and privacy protection – Guidance on managing information security risks, 2022, ISO/IEC 27005:2022