# The role of compliance in the operation of credit institutions

**Andrea Pelei[1] – Petra Benedek[2]**

**SUMMARY:** The aim of this article is to present a conceptual framework for compliance with legal and ethical standards in the business environment, with a particular focus on the role and current challenges of internal control. The paper describes systems and methods for developing effective compliance risk management strategies. The paper presents the importance of an organization's internal control systems through a literature review. It shows how compliance tools can be used to prevent harmful processes and how to deal with abuses such as money laundering. Finally, the article outlines new compliance challenges, such as the indirect effects of the Russia-Ukraine war and the challenges of implementing sanctions.
**KEYWORDS:** compliance management, internal control, money laundering, sanctions
**JEL-CODES:** G21, G23
**DOI:** https://doi.org/10.35551/PFQ_2024_1_3

## Introduction

The perception of companies is strongly influenced by their ability to adapt to the given legal environment and social norms, without which their activities would be impossible. Over the last decades, compliance management methods have been increasingly used in a growing number of sectors to comply with legislation. In Hungary, this approach was predominantly used in the banking sector until 2019, but pursuant to the Government Decree 339/2019 (23.12.2019), it is now mandatory to employ a compliance specialist in majority state-owned and municipal companies, the details of which are set out in the Decree.

Alongside national authorities, EU regulations and directives together create a constantly changing legislative environment, and following and ensuring ongoing compliance has become a top priority for all organisations. At the same time, even without legal constraints, business owners and managers are increasingly recognising

1 MBA, Compliance Officer in banking sector
2 PhD, Department of Management and Business Economics, Faculty of Economic and Social Sciences, Budapest University of Technology and Economics, Budapest, assistant professor

that efficiency and legality must go hand in hand in running their businesses – transparency of business operations is essential to their long-term success (risk management and compliance)[3] .

The first chapter of the paper presents the literature review. This is followed by a discussion of the role of compliance in internal control and then specifically on anti-money laundering activities. The paper concludes with a discussion of current challenges in compliance management and conclusions.

## Literature review

In general terms, control is a complex and sophisticated process that helps to identify sources of risk to the operation of an organisation. Risk is defined as any factor that may impede the organisation's ability to carry out its mission in an orderly, ethical, economical, efficient and effective manner (Tóth et al., 2021).

In the business risk management's literature, the term control is used to refer to the management of risks identified in the course of business (IAASB, 2022). According to the International Organization of Supreme Audit Institutions (INTOSAI), control is an activity by management that is designed to manage risks, promote the achievement of objectives and establishes as a principle that internal control is designed to promote standards of conduct and ethics and to prevent fraud and corruption. (Kovács, 2009) The European Court of Auditors defines internal control as "a process implemented by an organisation's board of directors, management and other staff, designed to provide reasonable assurance that the organisation has achieved its objectives in terms of its operations, its reporting process and its compliance with standards" (European Court of Auditors, 2016, p. 29).

To put this control into practice, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), established in 1985, developed a comprehensive, integrated risk management framework on the joint initiative of its member organizations, which was published in 1992 and became known as the COSO framework. The COSO control environment is characterised by its coverage of the entire organisation of the company (comprehensive), its application linking corporate governance with operational risk and the monitoring of regulatory compliance (integrated control). The COSO framework has become one of the most well-known internal audit methodologies in the world, used in both the competitive sector and in public administration.

3 In general, historically, risk management – which long predates institutionalised compliance monitoring – and compliance management in banking have evolved in organisationally separate ways. Risk management delt with risk identification and mitigation, while compliance monitors delt with compliance monitoring. In the past, these two activities were typically treated as separate disciplines by researchers, but there is now a general consensus that an integrated approach is the more appropriate.

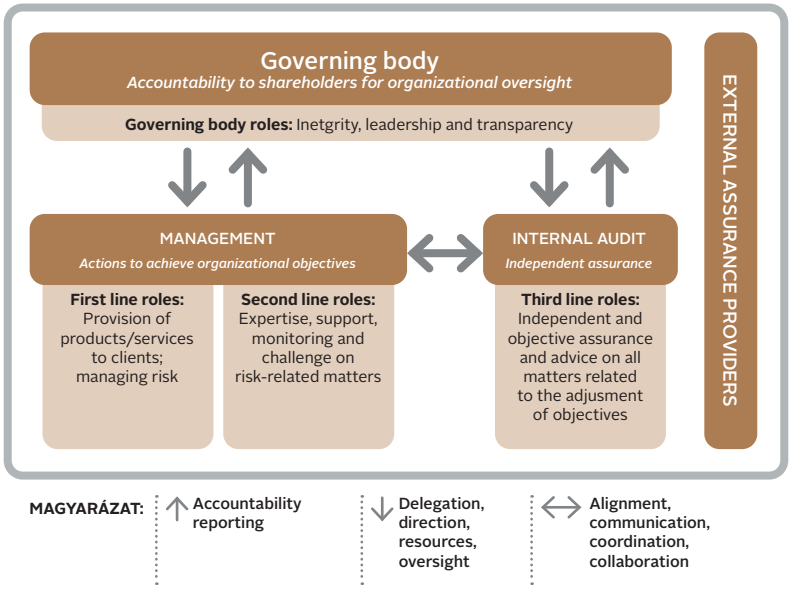
The COSO model was last revised in 2013 and the new framework includes 17 principles that are essential for internal control. The new 2013 framework is characterised by a greater emphasis on management concepts (COSO, 2013).

The six principles of the model underpin risk-based decision making, which includes analysis, planning, action, monitoring, review, and considers uncertainty factors affecting objectives. Although, the internal audit is accountable to and informs management, however, in terms of operation, it is independent of management and subordinate to it in the organisational hierarchy, i.e. it cannot exercise supervisory authority over management, since only the governing body is entitled to do so.

The relevant international standard for compliance is the ISO 37301:2021 Compliance management systems (CMS). It replaces and complements the previous ISO 19600:2014 guidelines and is particularly well suited to serve the standardisation trends in the compliance field. Its requirements are applicable regardless of the industry.

A theoretical analysis of the issue of internal control would not be complete without a document on the "three lines of defence model of Governing Body" published in 2013 by The Institute of Internal Auditors (IIA, 2019). As shown in Figure 1, the primary difference between the three pillars of the model is their "independence", i.e. their distance from the Governing Body.

**Figure 1: The IIA Three-Lines Model**




Source: IIA (2019, p. 5.)

In Hungary, the importance of internal control started to increase after the regime change, as companies operating on the basis of socialist economic principles realised that the lack of internal control in the real market environment had a

fundamental impact on organisational competitiveness (they realised the need for risk management, and were "forced" to follow the regulatory changes and ensure continuous compliance with them). Today's internal control systems are based on the triad of management control, control built into the process of activities and independent internal control. Practitioners typically follow international practice in designing organisational internal control systems, based on the recommendations of INTOSAI (International Organization of Supreme Audit Institutions), COSO and COBIT (The Control Objectives for Information and related Technology) (Ministry of National Economy, 2017).

Overall, it can therefore be said that in the 21st century, both internal control and internal audit have become direct support tools for governing body and cover the institutionalised monitoring of risk management and compliance in an integrated way. They share the common characteristic that control systems provide the necessary information for governance to management and leadership (Zéman, 2017).

## Compliance as a tool for internal control

The compliance departments of international credit institutions and their subsidiaries have a control mechanism in place to monitor the management of non-compliance risk. They focus their activities and priorities primarily on those areas, standards, processes and procedures where the risk of non-compliance is greatest. Thus, the credit institution's compliance control system shall aim to identify, measure, assess, monitor, manage and mitigate risks appropriately and systematically.

The compliance area identifies the risk of potential breaches of legislation and other non-compliances, and supports the development of internal procedures that provide protection against compliance risks at the organisational level. Compliance also advises business areas on acceptable behaviour and practices and monitors regulatory changes. In addition to the above, compliance monitoring also carries out reporting tasks for more effective controls. As a line of defence, the compliance assurance area plays both a supportive and a control role in mitigating risks.

In business and finance, compliance laws, rules and standards generally cover issues such as adherence to appropriate standards of market conduct (e.g. competition rules), managing conflicts of interest, treating customers fairly, ensuring transparency for customers and ensuring consumer protection regulation. These typically cover specific areas, such as the prevention of money laundering and terrorist financing, but may also include tax laws on the structuring of banking products or customer advice. (Domokos, 2019) The compliance function is responsible for preventing and detecting external and internal fraud and corruption, combating money laundering and terrorist financing, treating customers fairly, consumer protection, etc. (Isayev, 2021)

Collaboration with staff and experts in the areas of the credit institution (legal and human resources, quality assurance and internal control), as well as the development and maintenance of a compliance culture that encourages a positive attitude towards risk management and compliance within the organisation, and a robust

and comprehensive internal control framework, are key to the performance of these tasks. Communication, training and people development, as well as performance management and governance sensitisation, are key factors in the implementation of a compliance culture.

In the life and operations of a credit institution, 'compliance' can take many forms, such as ethical behaviour towards customers, compliance with competition rules, acceptance of gifts, harassment at work and any other incidents that may compromise the integrity of the organisation. In relation to the risks mentioned above, it is not enough to identify and manage them appropriately, but it is also essential to have these processes and responsibilities in place. One of the tools for this can be a Code of Ethics, which not only sets out the values and expectations derived from the credit institution's own mission, and vision, but also incorporates recommendations made by supervisory bodies and guidance from ISO standards and guidelines.

Compliance activity is often referred to in domestic financial terminology as the "compliance assurance function". A recommendation issued by the Magyar Nemzeti Bank in 2022 classifies the compliance function as one of the internal lines of defence of banks, defining its tasks as operational in nature (Magyar Nemzeti Bank, 2022).

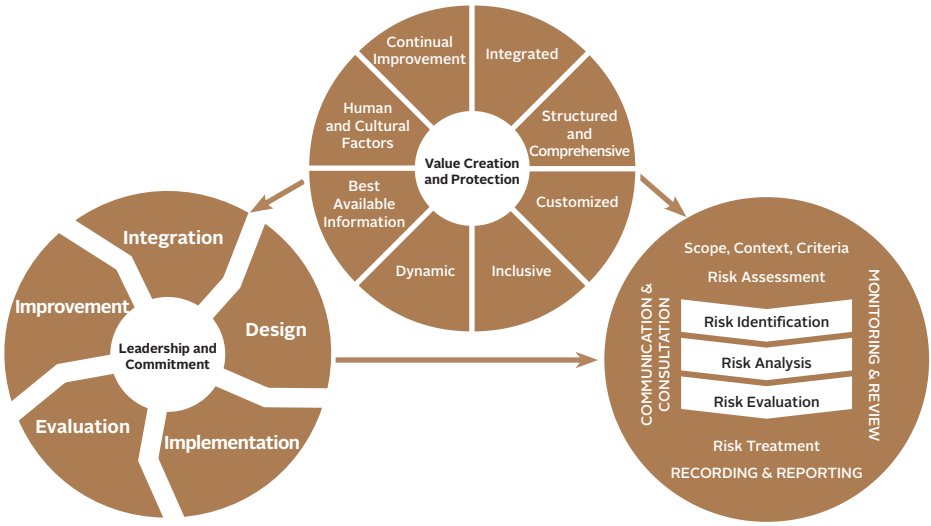
Increasing compliance requirements call for a strategy that integrates risk management and corporate objectives. (Kendall, 2021) The complexity of the risk environment and the penalties for non-compliance make a thorough assessment of exposure to compliance risk essential.

Compliance has an impact on operational risk and risk has an impact on compliance, since what happens within the compliance programme directly affects operations. Compliance consists of a framework of legal, regulatory or contractual requirements and the controls implemented to meet these obligations (Schmoeller, 2022)

A risk analysis provides the analyst with the opportunity to assess the nature and severity of potential hazards (hazard identification), to map the risk objects at risk (vulnerability assessment) and to gain insight into the potential impact of the sources of hazards (impact analysis). The impacts can be manifold, and in the economic field can mainly result in business interruption, loss of customer and partner confidence, or even the imposition of penalties and fines (Székely, 2015).

The most common risk factors in the life of companies are technological hazards, financial impacts on operations, activities related to the performance of a job, and environmental damage. Risk management can be helped by risk management governance systems that help identify risks (Balogh, 2011).

**Figure 2: The process of risk management and its relationship with risk management**




Source: ISO 31000:2018

Within the overall process of risk management, a "core area" can – and should – be distinguished, which is capable of producing a complete risk profile of the company (Figure 2). This core area is commonly referred to as risk assessment. In this case, the first task is to identify, analyse and, last but not least, weight all the risks that pose a threat to the organisation's operations. Once the potential risks have been identified and analysed, the second step is to formulate possible interventions and responses. This activity is also referred to as risk strategy. The reference to the strategic level stems from the fact that the decision on how to manage risk is taken by the top management of the organisation. Strategic responses can include avoiding, reducing, transferring, sharing or bearing (accepting) risk (Mesterházy, 2016).

The components of a Compliance Risk Assessment (CRA) – unheard of more than a decade ago – are now ubiquitous. They help to understand the full range of risk exposures, including the likelihood of a risk event occurring, the causes of its occurrence and the potential severity of its impact. They identify the inherent risks, list the controls in place to mitigate the risks, and code the resulting residual risk calculations as high, medium or low in terms of potential financial, regulatory and public reputation damage to the credit institution (Benedek, 2014).

Banking has always been a risky area of service provision. Recognising this, the legislator has made the granting of a banking licence subject to a number of financial, material and other conditions, irrespective of the country. The US model emerged in the life and activities of domestic credit institutions around the 2000s in such a way that the establishment of a compliance department was not required by domestic

legislation, but was made inevitable by the US model requirement. This led to a tendency for the top management and senior management of domestic credit institutions to view compliance as something unnecessary and cost-increasing, interpreting it as a kind of "American fad" (Benedek, 2019). The legislator's goal with the change was to strengthen internal control in banking operations and to help compliance to maintain effective risk management and governance functions of banks.

It is reasonable to not that some compliance risks may be specific to a particular industry or organisation (e.g. employee safety regulations for manufacturers or pharmaceuticals, environmental regulations, etc.), while other compliance risks are general regardless of the industry, such as conflict of interest rules, labour protection, data protection and document retention rules (Balogh, 2015).

Banking risk management is also important because credit institutions play an inescapable role in the functioning and operation of economic systems (Juhász, Kovács, 2016).

Compliance risks in banking affect legal, financial, business and reputational indicators (Jacsó, 2019a), while in terms of their nature, they may be residual risks that persist beyond the inherent risk. Residual risk is the actual risk to which the bank is currently exposed, given the controls already in place and their effectiveness. (Kaminski & Robu, 2016).

With regard to the detection, screening, analysis and management of compliance risks, the effective compliance function operates monitoring systems or receives information from systems operated by other professional areas. The monitoring systems functions shall also ensure compliance in areas, products and services where the number of incidents or the complexity of the organisational structure does not allow for the detection and management of compliance risks. The proliferation of such systems across the organisation has the potential to increase understanding and acceptance of the compliance function (Kovács, Marsi, 2018).

The practice shows that both in the case of domestic and foreign credit institutions, there are ongoing discussions between the financial supervisors and the compliance managers of the credit institution on the practical application of the requirements and the relevant rules, as the common goal is to comply with and enforce the rules (Dniestrzanska, 2015).

According to Ernst & Young's 2021 Recommendation states that due to the nature and level of risk inherent in their business activities, complex banking organisations should have a compliance risk management framework in place to identify, monitor and effectively control compliance risks across their entire organisation. As a result, compliance risk management has become a key business concern worldwide (Lavine, Ricko, 2021).

A successful compliance risk management programme includes at least the following elements:

1. Active board and senior management supervision. It is critical that senior management sets an example, risk approach and awareness in the organisation.
2. Effective policies and procedures. Regular recalculation of compliance risks based on new information (to ensure timeliness).

3. Compliance risk analysis and comprehensive controls.
4. Effective compliance monitoring and reporting.
5. Independent testing. Assessment and evaluation of compliance risk mitigation activities. (Sound and..., 2022)

The five elements of the Compliance Risk Management Programme offer comprehensive solutions that enable organisations to adopt a customised risk-based approach.

Specifically for credit institutions, in addition to the compliance policies and procedures already in place, the following elements may be useful to ensure compliance (Duncan, 2022):

1. Designation of the person responsible (accountable) for compliance
2. Easy access to policies and procedures
3. Communication of changes and amendments
4. Training
5. Good governance and building a compliance-conscious organisational culture.

In the context of compliance, it is also necessary to talk about the Compliance Management System (CMS). CMS is in fact a system of activities that brings together the activities that result in the employees of the organisation becoming aware of and recognising the legal, ethical and professional expectations necessary for the performance of their job duties. (Kocziszky, Kardkovács, 2020).

It is always a potential risk for companies that their employees do not have sufficient knowledge of the rules that apply to them or their area of expertise, so compliance management should therefore also treat education as a priority. Changes in the regulatory environment or staff turnover can affect company operations to an extent that can be an ongoing challenge for the organisation, but risks can be mitigated by organising training to an appropriate extent (Balogh, 2015).

Given that compliance officers perform compliance assurance activities as part of the internal lines of defence, they must work in an effective and balanced manner with the other departments of the bank that have control functions. These may include, but are not limited to, internal audit, bank security, IT security, legal, data protection, operational risk management, consumer protection, and units responsible for preventing or identifying money laundering and anti-fraud activities (Hungarian Banking Association, 2017).

General experience suggests that the systemic "operation" of compliance within a company creates a positive organisational culture that values compliance, ethical behaviour, transparency and integrity. In this context, leadership by example is valued, and leaders contribute to the development of a perception and internal attitude within an organisation that compliance is everyone's responsibility (Duncan, 2022).

In Hungary, as in other countries in Central Europe, the number of corporate abuses is higher than in Western countries, so it is necessary for Hungarian organisations to recognise that compliance management activities need to be

embedded in the corporate culture and that they need to build an effective control environment and monitoring system (PwC, 2018).

In traditional legislation, breaking the law is usually followed by criminal proceedings, with the law sanctioning the crime. In recent years, however, legislation has sought to make these processes more proactive, so that the legal system is not only able to react to violations, but also to focus on preventing and avoiding them. These laws, which are designed to prevent illegal or immoral corporate operations, are also known as compliance rules (Ambrus, 2020).

Today, more and more organisations are aware that it is not enough to avoid infringing behaviour, but that it is also necessary to beware of suspicions of it. Previously, this used to be a fundamental requirement only for money laundering activities, but now it is also necessary to be mindful of this requirement when implementing the ethical values of organisations (MOL Group, 2021).

Social and legal norms therefore define for economic operators what can and cannot be done in their operations, but not how to get the company as a whole to do what it is allowed to do in their daily activities. The task of compliance management is to provide answers to these questions, to set frameworks and to deepen these norms in the corporate culture (Inzelt, Bezsenyi, 2021).

Thanks to this recognition, but also thanks to international standards (expectations), the application of compliance management has become a common practice and part of the daily activities of long-established market players, such as large companies. However, for emerging market players, such as small and medium-sized enterprises (SMEs), compliance monitoring is still a rare occurrence in an international context. This is not primarily due to a lack of recognition, but rather to the fact that enterprises have fewer financial and personal resources, a lack of sector-specific knowledge and, in essence, less time to develop their knowledge of the regulatory background. But presumably, the need to monitor the business from a compliance perspective is not yet present in the SME managers (the focus is elsewhere: market access, survival, etc. and a possible regulatory action is a distant threat) (Kelecsényi, 2016)

## The role of compliance in the fight against money laundering

Practical experience shows that the majority of violations committed by companies are crimes related to money laundering. The income and/or revenue proceeds from money laundering not only distort the market, but also indirectly "trickle down" into politics, thus posing a threat to the purity of public life (Bálint, 2016). The complex nature of money laundering can be blamed for the fact that the fight against money laundering is a serious challenge for both legislature and law enforcement authorities (Ambrus, Farkas, 2019).

The purpose of money laundering is to deliberately conceal the origin of the proceeds of illegal activity or crime (Ambrus, Farkas, 2019). The term emerged in the early 1970s in the context of the Watergate scandal. In Hungary, money laundering

was introduced into the Criminal Code in 1994. Criminal gangs try to "cleanse" the proceeds of crime even if this means losing a significant part of the amount invested. Their activities are supported by a high level of conspiracy, a strong technological background and, not infrequently, a powerful political lobby. (Szendrei, 2018)

Money laundering is a lucrative business, estimated by the IMF to account for 2-5% of the GDP of all countries in the world (IMF, 2021) Money laundering can be considered a service without real products, and aims to prevent the identification of the origin of illicit funds. This illegality also lies in this.

In the European Union, the fight against money laundering is of particular importance as it is a powerful tool to prevent the financing of terrorism. For this reason, Community rules have been significantly tightened since 2018. These measures do not only focus on the movement of fictitious funds, but also set out controls that credit institutions must carry out in high-risk countries. In addition, the exchange of information between credit institutions is accelerated and the responsibilities of financial supervisory authorities is strengthened. (Kozák, 2021).

There is an increasing risk that means of payments are shifted to the virtual space, their tracking becomes more difficult, and that criminals continue their activities by exploiting the system's shortcomings and legal loopholes. Community legislation is trying to close these loopholes, so in 2019 the Council of Europe developed strategic priorities and action plans to help it fight money laundering more effectively. These directives unify European regulation, creating an EU-level supervisory authority with direct supervisory powers (Council of Europe, 2020).

Money laundering compliance is a well-regulated and distinct area in the European Union, with a high degree of uniformity and consistency across Member States due to harmonisation. Preventive compliance tools are given a prominent role in the field of money laundering. The two most important preventive measures in the EU directives are customer identification measures and the obligation to report suspicious cases. In 2001, the Anti-Money Laundering Directive II extended and fixed the scope of the actors subject to these obligations, and in the Anti-Money Laundering Directive III, as a further tightening, traders above € 15,000 were also covered. This Directive introduced the risk-based regulatory model in the anti-money laundering instrument regime. In 2015, the Council of Europe adopted the Money Laundering Directive IV, which was intended to make the previous system more effective and is considered one of the most important tools in the fight against money laundering; it focuses on the reporting of suspicious transactions. Under the provisions of the Directive, each Member State is required to establish an independent and autonomous Financial Intelligence Unit (FIU) responsible for the prevention, detection and effective combating of money laundering and terrorist financing. The Anti-Money Laundering Directive IV was amended in 2018 to reflect the latest trends in money laundering offences and the rapidly changing nature of the threats and risks. (Jacsó, 2019b).

In line with the European Union Directive 2018/1673, Article 53 of Act XLIII of 2020 amending the Act on Hungarian Criminal Procedure and other related acts has completely redefined this type of offence with effect from 1 January 2021.

## Current challenges in compliance management

The coronavirus epidemic, which went global in spring of 2020, presented business with a new challenge, as the Covid-19 closures have rendered their business processes inoperable. The dominance of on-line customer relationships and the shift to home office working meant that organisations had to adapt their operating models to accommodate the needs of remote workers, customers and suppliers virtually overnight. This has been a challenge not only from a digitalisation and technology perspective, but also from a corporate security and risk management perspective. (Schmoeller, 2022).

According to McKinsey's global survey of business leaders in autumn 2020, companies have accelerated their interactions with customers and the supply chain, as well as the digitisation of their internal operations, by three to four years. (LaBerge et al., 2020). The proportion of digital or digitally supported products in their portfolios has accelerated at a staggering rate. The research came to the conclusion that the key to companies' competitiveness in the new business and economic environment shaped by Covid-19 is a reconsidered business strategy and operational practice. Most executives have recognised the strategic importance of technology and innovation for customer satisfaction and cost efficiency. Leaders of companies that responded successfully to the crisis reported a number of new organisational capabilities (e.g., more advanced technology, exploring and experimenting in new ways, openness to innovative solutions) that they did not have before the pandemic. (LaBerge et al., 2020)

According to the Ernst & Young Global's 2021 global information security survey, 77% of business leaders reported a significant increase in the number of dangerous external cyber-attacks, such as ransomware, in the 12month period prior to the survey. Another interesting finding of the survey is that despite the increased cybersecurity pressure, 81% of companies were still forced to ignore or avoid cybersecurity protocols, otherwise the negative impact of Covid-19 (e.g. insufficient budget, complex regulations, uncertain operating environment) would have pushed the organisation to the limit of inoperability. Only one in ten business leaders believed that their own cyber defence measures implemented by the organisation would protect the company from a serious, more damaging cyber attack from outside. (Burg et al., 2021)

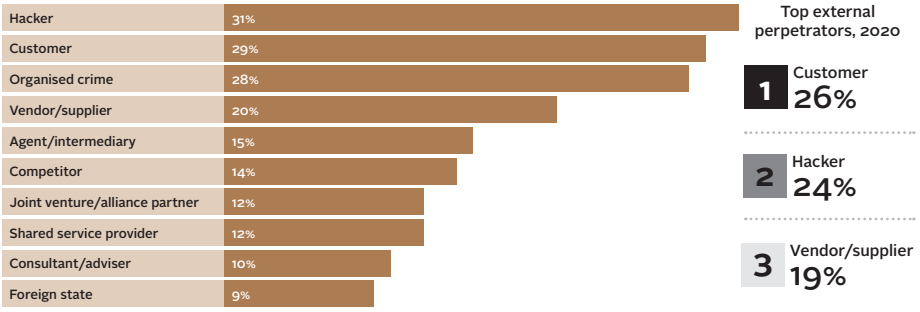
In the business sector, according to the PwC's 2022 report, the coronavirus epidemic has increased security risks in the provision of financial services in two ways (PwC, 2022). On the one hand, it has amplified the vulnerabilities that were already present in the life of banks and other credit institutions before Covid-19. However, the shift to the home office and the digitalisation of business and the shift of its focus to the online space have opened the door to new, unprecedented sources of risk in addition to the existing ones.

The main risks in business service provision include client fraud and risks arising from changes in or insufficient knowledge of the legal environment (Ulfkotte, 2013).

According to PwC's 2022 research, the real threat to a business comes from where it least expects it (PwC, 2022), such as suppliers, business partners, external

consultants brought in for their expertise (Figure 3). Market competitors undoubtedly represent a risk, but the level of danger can be said to be moderate. It is clear that the scope of the compliance function has now extended far beyond money laundering and that a good compliance manager needs to think in a complex way about the potential threats to the organisation's operations.

**Figure 3: Types of external offenders in 2022**




Source: own editing based on PwC (2022)

How can the attention of company managers be drawn to the importance of cyber defence, how can they be made more aware that IT security protocols are not necessarily "bad", but are strategic to the effective operation of the business? The answer may lie in the education function of compliance functions and the potential target groups for various internal training and education sessions include top managers. In the 2021 Survey of Chief Information Officer (CIO), respondents cited a number of challenges that have complicated their governance, risk and compliance (Government Risk Compliance) efforts in today's environment, which include (Schmoeller, 2022):

1. Limited resources (42%). Responding to risks is quite resource intensive.
2. New or changing regulation (19%). The global compliance environment is becoming increasingly complex. Completely new areas such as data management and data protection are becoming increasingly important.
3. Monitoring and maintaining compliance (15%). The increased volume and complexity of compliance makes it increasingly difficult to manually manage data and gather evidence to demonstrate that audits are designed and effectively carried out in accordance with compliance requirements.

Many organisations face all three challenges simultaneously, exacerbating the complex task of effectively managing information security, risk and compliance. (Schmoeller, 2022).

Since 2022, the European Union has imposed a series of sanctions against Russia and Russian-interested credit institutions. The European Central Bank (ECB) is not responsible for enforcing sanctions against Russia. The ECB does not apply these sanctions and does not monitor compliance by Member States, but Member States

are responsible at national level for implementing and monitoring compliance with the various sanctions regimes. Meanwhile, individual Member States are responsible for identifying breaches of sanctions applicable in the European Union and imposing sanctions where necessary. Thus, the ECB primarily only monitors the impact of sanctions on banks (European Central Bank, 2022a).

At national level, there is no single authority that performs this control function, but three different organisations in Hungary have the competence to perform this function (Table 1).

**Table 1: Hungarian agencies responsible for enforcing sanctions against Russia**

| Type of sanction | Competent body in Hungary |
|---|---|
| Trade restrictions | Government Office of the Capital City Budapest Department of Trade, Defence Industry, Export Control and Precious Metal Assay |
| Travel ban | National Directorate-General for Aliens Policing |
| Financial sanctions | National Tax and Customs Administration Anti-Money Laundering and Counter-Terrorist Financing Office |

Source: own editing, based on European Central Bank (2022b)

Sanctions against Russia are monitored by the European Banking Authority. The banks themselves are primarily responsible for implementing and monitoring compliance with the various sanctions regimes. In problematic cases, it is for the relevant competent national authority to decide whether the sanctions regime has been breached. In such a case, the competent authority may, if it finds a breach, act on its own competence, for example by imposing a fine, in the event of a violation of the law. In addition, a breach of sanctions can trigger criminal investigations and possible legal action, as well as cause significant reputational problems for credit institutions. (Pelei, 2022).

## Conclusions

The application of compliance management is still mainly the domain of large companies. In the SME sector, however, the application of compliance management is very low, not mainly because of a lack of awareness but because of the limited financial and human resources available. For this reason, there are many misconceptions in the wider public about the true nature and meaning of compliance (Kelecsényi, 2016).Compliance tools may vary across industries and even at the enterprise level (there is no one-size-fits-all compliance programme that can be presented as best practice), but compliance systems, when tailored to the specific company/organisation, can be successfully applied in any sector of the competitive sphere, in non-profit sectors, and even in state administration.

Compliance is no longer just about meeting the rules, but also about the whole corporate culture that values compliance and that permeates its policies and procedures. Truly competitive companies have recognised that breaching legal rules or social norms can put them at a serious competitive disadvantage and that the cost of compliance management pays off in the long run.

Today, the financial sector is the leader in the application of compliance management. In the banking sector, compliance risk arises when there is a possibility of breaching legal or ethical standards. New banking products, increased government scrutiny and an increased focus on compliance requirements are leading to higher risks and more comprehensive and complex rules and regulations. In today's stringent regulatory business environment, where new rules and regulations are coming into force at an unprecedented pace, keeping abreast of regulatory changes and ensuring ongoing compliance has become a top priority for all credit institutions. ■

## References


1. Ambrus, I. (2020). A compliance alapkérdései. https://mersz.hu/ambrus-farkas-a-compliance-alapkerdesei//, I. és II fejezetek.
2. Ambrus, I., Farkas, Á. (2019). A compliance alapkérdései – az etikus vállalati működés elmélete és gyakorlata. Budapest: Wolters Kluwer Hungary Kft..
3. Bálint, P. (2016). A pénzmosást megelőző alapbűncselekmény dilemmái. Belügyi Szemle, 65-75.
4. Balogh, A. (2011). Kockázatmenedzsment és kockázatértékelés. Magyar minőség, 6-14.
5. Balogh, M. (2015). A munkaügyi compliance audit. Budapest: Wolters Kluwer, I-III fejezetek.
6. Benedek, P. (2014). A vállalati compliance értékelése. Vezetéstudomány – Budapest Management Review, 29-39.
7. Benedek, P. (2019). Compliance menedzsment a pénzügyi szolgáltatásokban. Munkaügyi Szemle, 41-51.
8. Burg, D., Hussain, A., Watson, R. (2021). How do you rise above the waves of a perfect storm? The EY Global Information Security Survey 2021. https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm
9. COSO (2013). COSO Framework 2013 for Internal Controls and Management Responsibilities – By Compliance Global Inc: https://www.academia.edu/11623304/COSO_Framework_2013_for_Internal_Controls_and_Management_Responsibilities_By_Compliance_Global_Inc
10. Dniestrzanska, E. (2015): Monitoring of Compliance Risk in the Bank. Procedia Economics and Finance, 800-805.
11. Domokos, L. (2019): Ellenőrzés – a fenntartható jó kormányzás eszköze. Budapest: Akadémiai Kiadó, 2. fejezet.

12. Duncan, C. (2022): Ensure Compliance With Bank Policies and Procedures. https://www.alert-software.com/blog/ensure-compliance-with-bank-policies-and-procedures
13. Európa Tanács. (2020). Küzdelem a pénzmosás és a terrorizmusfinanszírozás ellen. https://www.consilium.europa.eu/hu/policies/fight-against-terrorism/fight-against-terrorist-financing/
14. Európai Számvevőszék. (2016). Különjelentés. Az Európai Bizottság szervezetirányítási rendszere: helyes gyakorlatok? (az EUMSZ 287. cikke (4) bekezdésének második albekezdése alapján). https://www.eca.europa.eu/lists/ecadocuments/sr16_27/sr_governance_hu.pdf
15. European Central Bank. (2022a): FAQs on Russia-Ukraine war and ECB Banking Supervision. https://www.bankingsupervision.europa.eu/press/publications/html/ssm.faq_Russia_Ukraine_war_and_Banking_Supervision~8360ccdf6f.en.html
16. European Central Bank. (2022b). National competent authorities for the implement of EU restrictive measures (sanctions). https://finance.ec.europa.eu/system/files/2023-11/national-competent-authorities-sanctions-implementation_en.pdf
17. IAASB (2022). 2022 Handbook of the International Code of Ethics for Professional Accountants. https://finance.ec.europa.eu/system/files/2023-11/national-competent-authorities-sanctions-implementation_en.pdf
18. IIA. (2019). Az IIA Három Vonal Modellje – A "három védelmi vonal" aktualizált verziója. https://preprod.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-hungarian.pdf
19. IMF (2021): IMF and the Fight Against Money Laundering and the Financing of Terrorism. https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing
20. Inzelt, É., Bezsenyi, T. (2021). A vállalati bűnözés jellemzőinek megértése: elméleti megfontolások és empirikus kutatás eredményei alapján. Budapest: ELTE Állam- és Jogtudományi Kar, IV. fejezet..
21. Isayev, F. (2021). Compliance Function as a Pillar of Modern Corporation. https://assets.kpmg.com/content/dam/kpmg/az/pdf/ArticlesNPubs/compliance-function-as-a-pillar-of-modern-corporation.pdf
22. ISO (2018): ISO 31000:2018 Risk management — Guidelines
23. Jacsó J. (2019a): A compliance fogalmáról és szerepéről a gazdasági életben. Miskolci Jogi Szemle, 82-91.
24. Jacsó J. (2019b): A pénzmosás compliance hazai és európai dimenzióban a társadalmi innováció tükrében. https://www.mjsz.uni-miskolc.hu/files/6568/38_jacsojudit_t%C3%B6rdelt.pdf, 3.2. fejezet.
25. Juhász, Z., Kovács, R. (2016). A banki kockázatmenedzsment új irányai a hazai és a nemzetközi gyakorlatban. Gazdaság és társadalom : társadalomtudományi folyóirat, 28-50.

26. Kaminski, P., Robu, K. (2016): A best-practice model for bank compliance. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-best-practice-model-for-bank-compliance
27. Kelecsényi R. B. (2016): A kis-és középvállalkozások és a versenyjog kapcsolata az ideális megfelelési politika érdekében. Versenytükör, 16-30.
28. Kendall, K. (2021). A kockázatmenedzsment növekvő jelentősége. Minőség és megbízhatóság, 22-26.
29. Kocziszky G., Kardkovács K. (2020). A compliance szerepe a közösségi értékek és érdekek védelmében. Budapest: Akadémiai Kiadó, 3. és 4. fejezet..
30. Kovács L., Marsi E. (2018). Bankmenedzsment, banküzemtan. Budapest: Magyar Bankszövetség, 2. fejezet..
31. Kovács S. (2009). Az államháztartási kontrollok rendszere, belső kontroll, belső ellenőrzés a nemzetközi standardok és a vonatkozó jogszabályi változások tükrében. Egészségügyi gazdasági szemle, 12-18.
32. Kozák A. (2021). Pénzmosás compliance az ügyvédi tevékenység körében. Miskolci Jogi Szemle, 111-125.
33. LaBerge, L., O'Toole, C., Schneider, J., Smaje, K. (2020). How COVID-19 has pushed companies over the technology tipping point – and transformed business forever, survey. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
34. Lavine, J., Ricko, A. (2021). Bank regulatory compliance services. https://www.pwc.com/us/en/industries/financial-services/regulatory-services/bank-regulatory-compliance.html
35. Magyar Bankszövetség. (2017). A compliance (megfelelőség biztosítási) funkció működtetésének legjobb gyakorlata (Best Practice Kódex). https://www.bankszovetseg.hu/Content/alapdokumentumok/6_melleklet_Compliance_Best_Practice_Kodex_HUN.pdf
36. Magyar Nemzeti Bank (2022). A Magyar Nemzeti Bank 12/2022. (VIII.11.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról https://www.mnb.hu/letoltes/12-2022-belso-vedelmi-vonalak-ajanlas.pdf
37. Mesterházy, B. (2016). A vállalati kockázatmenedzsment alapjai és a kockázatkezelés gyakorlati előnyei. Magyar minőség, 30-56.
38. MOL Group. (2021). Etikai és üzleti magatartási kódex. https://molgroup.info/storage/documents/sustainability/mol_csoport_etikai_kodex.pdf
39. Nemzetgazdasági Minisztérium. (2017). Államháztartási Belső Kontroll Standardok és Gyakorlati Útmutató. Budapest: Nemzetgazdasági Minisztérium, II. fejezet.
40. Pelei, A. (2022). A compliance szerepe a pénzintézetek működésében. MBA szakdolgozat. Budapesti Műszaki és Gazdaságtudományi Egyetem, 46-48.
41. PwC. (2018). A gazdasági bűnözés konstans veszélyt jelent – 2018. évi felmérés a globális és magyar gazdasági bűnözésről és visszaélésekről. https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/gazdasagibunozes_hu_18.pdf

42. PwC. (2022). PwC's Global Economic Crime and Fraud Survey 2022. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
43. Schmoeller, D. (2022). Have a strong compliance program? Use it as a foundation for risk management. https://reciprocity.com/wp-content/uploads/2022/03/Reciprocity_white_paper_Compliance_Risk_Management.pdf
44. Sound and effective Compliance Risk Management in Banks (2022). https://www.metricstream.com/insights/effective_compliance_risk_management_banks.htm
45. Székely, C. (2015). Stratégiai kockázatmenedzsment = Strategic risk management. TAYLOR : gazdálkodás- és szervezéstudományi folyóirat, 103-118.
46. Szendrei, F. (2018). A szervezett bűnözés gazdasági háttere és a pénzmosás. Magyar rendészet: a Nemzeti Közszolgálati Egyetem Rendészettudományi Karának szakmai, tudományos folyóirata, 77-91.
47. Tóth, B., Rácz, A. T., Lippai-Makra, E. (2021). Belső kontroll és pénzügyi kockázatok vizsgálata a helyi önkormányzatoknál. Új magyar közigazgatás, 45-55.
48. Ulfkotte, U. (2013). Az amerikai lehallgatás célja a gazdasági kémkedés volt, ráadásul ezzel az európai szövetségesek is tisztában vannak. https://uzletihirszerzes.blog.hu/2013/10/11/az_amerikai_lehallgatas_celja_a_gazdasagi_kemkedes_volt_raadasul_ezzel_az_europai_szovetsegesek_is_t
49. Zéman, Z. (2017). A vezetői számvitel funkcionális kapcsolata a vállalati belső kontroll környezettel. Jura, 193-198.