

**Recommendation No 12/2022 (VIII. 11.) of the Magyar Nemzeti Bank
on setting up and operating internal lines of defence and on the management and control
functions of financial institutions**

I. Purpose and scope of the recommendation

In terms of ensuring reliable, cautious and prudent operation, the proper functioning of the supervised financial institutions' internal lines of defence is of utmost importance. The purpose of the recommendation is to formulate the expectations of the Magyar Nemzeti Bank (hereinafter: MNB) regarding financial institutions' lines of defence, and thereby to increase the predictability of law enforcement and foster the uniform application of the relevant laws.

-This Recommendation transposes the European Banking Authority's (hereinafter: EBA) Guidelines on Internal Governance (EBA/GL/2021/05)¹, published on 2 July 2021, the European Securities and Markets Authority's (hereinafter: ESMA) Guidelines on certain aspects of the MiFID II compliance function requirements ((ESMA35-36-1952) published on 6 April 2021², and certain provisions of the Joint Guideline of EBA and ESMA on the Assessment of suitability of members of the management body(EBA/GL/2021/06, ESMA35-36-2319)³, published simultaneously with this.

The Recommendation is addressed to entities domiciled in Hungary that are subject to the laws specified in Article 39(1) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank, and to branches of financial institutions in Hungary domiciled in a country outside the European Union or in another state party to the Agreement on the European Economic Area (third country) (hereinafter: "financial institutions").

The MNB also recommends to issuers to follow the supervisory authority's requirements outlined in the recommendation.

The MNB draws attention to the fact that with regard to the internal lines of defence of insurance and reinsurance companies, the MNB has also formulated special expectations, in addition to the general expectations of this recommendation, in MNB Recommendation No 17/2019 (IX. 20.) on the governance system of insurance and reinsurance companies.

The set of rules relevant to the subject matter of this recommendation are included in particular, but not exclusively, in the sectoral legislation. This recommendation does not fully refer back to

¹ [GL on internal governance under CRD_HU.pdf \(europa.eu\)](#)

² [guidelines on certain aspects of mifid ii compliance function requirements_hu.pdf \(europa.eu\)](#)

³ [EBA BS 2017 XXX \(Final GL on the assessment of suitability of MB members and KFH\).docx \(europa.eu\)](#)

the legal provisions when setting out the principles and expectations, but the addressees of this recommendation are of course still obliged to comply with the relevant legal requirements.

The recommendation is consistent with the requirements of the European framework for the operation of financial institutions.

This recommendation does not provide any guidance on data management and data protection issues, does not contain any expectations with regard to the processing of personal data and the requirements contained in this recommendation should not be in any way interpreted as an authorisation to process personal data. Data processing in the context of the fulfilment of the supervisory requirements set out in the recommendation should only be carried out in compliance with the data protection legislation in force at any time.

II. Definitions

1. For the purposes of this recommendation:

a) *sectoral legislation:*

1. Act XCVI of 1993 on Voluntary Mutual Insurance Funds,
2. b) Act XLII of 1994 on the Hungarian Export-Import Bank Plc and the Hungarian Export Credit Insurance Plc,
3. Act CXIII of 1996 on Building Societies,
4. Act XXX of 1997 on Mortgage Loan Companies and Mortgage Bonds,
5. Act LXXXII of 1997 on Private pension and Private pension funds,
6. the Act XX of 2001 on the Hungarian Development Bank Plc,
7. Act XX of 2001 on the Capital Markets,
8. Act CXVII of 2007 on Occupational Pension and the Related Institutions,
9. Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities (hereinafter: "Investment Services Act"),
10. Act LXXXV of 2009 on the Provision of Payment Services,
11. Act CXXXV of 2013 on the integration of cooperative credit institutions and the amendment of certain acts on economic matters (hereinafter: "Cooperative Credit Institutions Act"),
12. Act CCXXXV of 2013 on certain payment service providers,
13. Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter: "Credit Institutions Act"),
14. Act XVI of 2014 on Collective Investment Forms and their Managers, and on the Amendment of Financial Laws,

15. Act LXXXVIII of 2014 on the Business of Insurance (hereinafter: "Insurance Act"),
16. Act LIII of 2017 on the Prevention of and Combating Money Laundering and Terrorist Financing (hereinafter: "Anti-money Laundering Act"),
17. Government Decree No 79/2014. (III. 14.) on the organisational, conflicts of interest, business conduct and risk management requirements concerning UCITS managers,
18. Government Decree No 436/2016 (XII. 16.) on the detailed rules for the group supervision of insurance and reinsurance undertakings,
19. Regulation 575/2013/EU of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation 648/2012/EU (hereinafter: "CRR")
20. Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC
21. Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision,
22. Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)
23. Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive
24. Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (hereinafter: "IFR"),
25. Regulatory and implementing technical standards adopted under the mandates provided for in Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)
26. Regulatory and implementing technical standards issued under the mandates in the CRR,
27. Regulatory and implementing technical standards issued under mandates in Regulation (EU) No 596/2014 of the European Parliament and of the Council,
28. Implementing technical standards issued under the mandates in the IFR,

- b) *external service provider*: a service provider other than the financial institution, including a service provider within the same group or institutional protection scheme of which the financial institution is a member or which is a member of the financial institution;
- c) *money laundering and terrorist financing risk*: the term defined in subpoint f) of point 1 of MNB Recommendation No 1/2022 (I. 17.) on the assessment of the eligibility of the members of executive bodies and persons in key position [hereinafter: MNB Recommendation No 1/2022 (I. 17.)].

III. General principles

III.1 Structure of internal defence lines

2. The financial institution is expected to develop and operate internal lines of defence that facilitate
 - a) the prudent, reliable and efficient operation of the financial institution in compliance with the legislation and internal regulations;
 - b) the protection of the financial institution's assets as well as of owners' and clients' economic interests and social goals linked to the financial institution;
 - c) the smooth and efficient operation of the financial institution and the maintenance of confidence in it.
- A the most important function of the financial institution's internal lines of defence is to contribute to meeting these goals in a preventive and proactive manner by identifying and managing potential problems arising in the course of operation in the earliest possible phase, already at the time of occurrence or even before that, if possible, thereby guaranteeing the solution's speed and efficiency. The internal lines of defence act as a primary filter in the protective network guaranteeing the safe operation of the financial intermediary system.
3. The internal lines of defence of a financial institution consist of the responsible internal governance⁴ and the internal control functions, belonging to the second and third lines of defence, supplementing the controls integrated in the business processes (primary line of defence).
 4. Responsible internal governance is guaranteed by the financial institution by setting up and operating an adequate organisational structure, organisation and system of corporate bodies and by exercising management and supervision functions. The exercise of the management function includes administrative and representational tasks, while the exercise of the

⁴ Providing the terms in English reflects the MNB's efforts to ensure that the recommendation conveys the accepted international terminology to financial institutions in the most accurate way possible, covering the meaning of the term.

supervision function includes monitoring, control and surveillance tasks. Internal governance shall be interpreted as part of responsible corporate governance, the former being narrower in the sense that it does not extend to relationships with the owners and other stakeholders of the financial institution.

- A the risk control function and the compliance function should be classified as internal control functions belonging to the second line of defence, while the third line of defence comprises the internal audit function (hereinafter collectively: internal control functions).
-

III.2 Group operation

5. In the case of credit institutions, financial holding companies, mixed financial holding companies, investment firms, investment holding companies, insurance companies and reinsurance companies (hereinafter collectively: controlling financial institution) subject to consolidated supervision based on the legislation applicable to the sector, the MNB expects that internal lines of defence are established and operated also at group level and that the controlling financial institution establishes and operates a management and supervision function in relation to the internal lines of defence for the members of the group, irrespective of their domicile. To this end, it is essential that internal management and control practices within the group are based on the same principles – unless they are in conflict with local regulations relevant to any of the group members – and that the responsibility for this lies with the governing body of the controlling financial institution.
6. When designing and operating the internal lines of defence at group level, the MNB expects both the controlling financial institution and the group members that the special features of service provision and operation as a group, as well as the risks of the group as a whole and of the group members, are taken into consideration in all sub-areas (responsible internal management, internal control functions) that comprise the internal line of defence. Within the framework of this, upon making decisions the controlling financial institution shall also take into consideration the impacts on the group members, while the group members shall create an internal management and control environment that ensures that the decisions taken by the controlling financial institution do not jeopardise the safe management and operation of the group members, compliance with the legislation applicable to group members and the enforcement of ownership rights.
7. Key tools for the design and operation of the lines of defence at group level:
 - a) a group structure, organisational structure and operational structure (including the development of corporative bodies that ensure independence and appropriate checks and balances), responsibility, authority and reporting schemes in line with nature of the

business model and the special features, scope, complexity and risks of the service activities pursued,

- b) adoption and practical application of internal management and control policies at group level,
- c) exercising management and supervisory functions with regard to the internal management and control functions of the group members,
- d) developing and operating internal control functions at group level.

The detailed expectations on the group aspects of the development and operation of internal lines of defences are included in the respective sections of the recommendation.

- 8. When the parent company of a financial institution is a financial institution with registered office outside Hungary or it is the member of an international financial group in any other way, the MNB expects that – complying with the statutory requirements and the expectations of this recommendation – the development and operation of the financial institution's internal lines of defence are in line with and conform to the principles and solutions applied by the group.
- 9. In line with the Integration Act, the internal lines of defence of credit institutions operating as a member of the Integration Organisation shall be developed by the central body of the credit institutions' integration in the manner stipulated by the Integration Organisation.

III.3 Proportionality

- 10. The financial institution shall develop and operate its internal lines of defence and the individual elements forming part of those in compliance with the relevant laws and ensuring prudent operation, in line with the nature of the applied business model, the special features – including also the features inherent in the organisational structure – scope, complexity, risks of the services activity pursued by the financial institution and the group and its role in the financial intermediary system. Application bearing in mind the principle of proportionality equally applies to the internal policies, regulations, organisational solutions expected on the basis of the recommendation as well as the practices and procedures implemented.

With a view to enforcing the principle of proportionality, the financial institution shall develop its internal lines of defence particularly based on the following criteria: a) size of the financial institution or group;

- b) whether – if relevant – the financial institution qualifies as a small and non-complex institution under point 145 of Article 4(1) of CRR or as a large institution under point 146 of Article 4(1) of CRR;
- c) geographical location of the financial institution or group; magnitude of the activities pursued in the individual jurisdictions;

- d) legal form of the financial institution, including also whether the financial institution is a member of a financial group, and if yes, its weight within the group;
- e) whether the financial institution is a listed enterprise;
- f) whether the financial institution uses internal models to measure capital requirements;
- g) type of the activities pursued and services rendered by the financial institution or group; business model and strategy of the financial institution or group, also taking into consideration – if relevant – the result of the business model analysis (BMA)⁵; nature and complexity of the business activities, and the interaction between the business activities pursued by it, and organisational structure of the financial institution or group;
- h) risk strategy, risk appetite and current risk profile of the financial institution or group, taking into account the results of the ICAAP and ILAAP⁶ and ORSA⁷ assessments;
- i) ownership and financing structure of the financial institution or group;
- j) nature of the customers of the financial institution or group (e.g. retail customers, small businesses, public institutions, other financial institutions), the complexity of products and contracts;
- k) scope of activities and distribution channels using an external service provider (including services provided through own commercial networks such as intermediaries or branches);
- l) existing information technology (IT) systems, including continuity of service systems and outsourcing of activities in this area.

Furthermore, with a view to enforcing the principle of proportionality, an investment firm to which the CRR requirements are not applicable and which is not a small and unrelated undertaking, upon developing its internal lines of defence shall take into consideration the amount of the instruments held and managed by it, the volume of the customer orders managed, the volume of the daily trading turnover as well as whether it has a licence for holding customer funds or instruments.

The MNB highlights that the size or systemic importance of a financial institution is not in itself necessarily an indication of the degree of exposure to risk.

III.4 Other expectations

11. The MNB expects the financial institution to formulate the framework of internal lines of defence for the institution or the group in writing, including at least the elements specified in Annex 1.

⁵ <https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/modszertani-kezikonyvek/icaap-ilaap-bma-felugyeletifelulvizsgalatok>

⁶ <https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/modszertani-kezikonyvek/icaap-ilaap-bma-felugyeletifelulvizsgalatok>

⁷ <https://www.mnb.hu/letoltes/3-2016-ajanlas-sajat-kockazat-es-szavatulotoke-ertekeles.pdf>

12. The financial institution's governing body is expected to assess regularly (with the frequency and in the manner stipulated by the law or in the internal regulation, in respect of which the MNB regards it as good practice to perform the assessment at least annually) the financial institution's or the group's internal lines of defence, the structure and operation of the individual sub-systems forming it and to take any corrective measures as necessary in due course, and monitor those.
13. In connection with the development and operation of the internal lines of defence, the MNB recommendation formulates expectations with regard to the adoption and application of an internal policy in several places. As to the specific form of the internal policies the MNB deems a number of solutions acceptable. Accordingly, the individual policies may be formulated in an independent document or as part of other policies or internal regulation, rules of procedures, terms of reference, etc. On the other hand, the financial institution is expected to be able to demonstrate to the MNB that, in areas (e.g. appointment of senior executives, risk control, compliance) where the MNB expects the development of internal policies in addition to the statutory requirements, the objectives specified and followed, principles and key practices are clearly defined in advance. A further general expectation with regard to the policies developed by the financial institution or group is that they should be approved by a body with management or supervision functions, communicated within the organisation, reviewed regularly, with the frequency and in the manner prescribed by the law or by the internal regulation – in respect of which the MNB regards it as good practice to perform the assessment at least annually – and that the practices of the financial institution or group should be consistent with the established policies at all times.
14. In the recommendation, the MNB sets out its expectations regarding the financial institutions' internal lines of defence in a sector-neutral manner, despite the fact that the different sectoral requirements of the international and domestic regulatory framework often do not facilitate this. Accordingly, the recommendation seeks to summarise best practices for the operation of internal lines of defence, applied by the financial institution based on the MNB's expectations, complying with the applicable statutory requirements and in line with the principle of proportionality specified in point 10. The legislation applicable to the sector specifies identical or, in some cases, stricter requirements than those outlined in the recommendation for certain sectors, types of financial institutions and topics. Compliance with the latter takes precedence over compliance with the MNB's requirements.⁸
15. In line with the prevailing international practice, the recommendation differentiates management bodies by function, separating the body with governance function from the body with supervision function. In Hungary, the governing body is usually the executive board (in the case of funds, the board of directors), while the oversight body is the supervisory board

⁸ The recommendation draws attention to these in footnotes.

(in the case of funds, the audit committee).⁹ Where a financial institution does not have an executive board, the MNB expects the financial institution to apply the requirements outlined in respect of the governing body to the managing director exercising the statutory powers of the Executive Board.

IV. Responsible internal governance

IV.1 Principles

16. The MNB attaches key importance to the financial institution's developing and operating an appropriate internal governance system based on the best practices specified in the recommendation, as a factor that fundamentally determines the quality and safety of operations.
17. In line with the principle of proportionality specified in point 10, the MNB expects large, internationally active financial institutions with a wide range of activities to comply with higher organisational and governance requirements compared to smaller financial institutions with less complex activities that are internationally inactive and operating only in a domestic environment.

IV.2 Organisational and operational framework

IV.2.1 Organisational structure and organisation

18. The MNB expects the financial institution or group to pursue its operation within an organisational and operating structure laid down in writing that provides an adequate basis for the effective and secure management of the financial institution, group or outsourced activities and for the exercise of supervision and control functions. In this context, the financial institution is expected to have an organisational and operational structure that facilitates and supports the governing body in the understanding and efficient management of risks affecting the financial institution or group, and the MNB in carrying out its micro- and macroprudential oversight activities.
19. According to the MNB's expectation the reporting lines and the division of responsibilities and powers within the financial institution, group and in respect of the outsourced activities should be adequately regulated and documented, clear, precise, straightforward, transparent, coherent, and they should support the flow of information, reporting and

⁹ In the Credit Institution Act, the body with governance function corresponds to the executive body with governance powers, while the body with oversight function corresponds to the executive body with supervisory powers.

control within the organisation, the correction of shortcomings, the prevention of money laundering and terrorist financing, and should be able to prevent, ensure the prevention and management of conflicts of interests and powers specified in point IV.9, and it should be possible to comply with and enforce those. The development of the foregoing, communication of those to the employees and its continuous operation shall be the primary responsibility of the financial institution's body with governance function.

20. Where the business reporting lines do not correspond to the legal structure of the financial institution or group, the MNB expects the financial institution to ensure that tasks and powers of the individual areas are clearly defined and transparent.
21. The governing body of the financial institution is expected to know and understand the organisational and operational structure of the financial institution or group, and to ensure that the organisational and operational structure is consistent with the financial institution's or group's strategy, risk appetite, risk profile and its role in the financial intermediary system and that the organisational and operational structure is covered by the risk management system. The management of the financial institution is also expected to understand the purpose and risks of the applied organisational, operational and group structure.
22. The MNB expects the organisational and operational structure of the financial institution and the structure of the financial group to be reviewed on a regular basis, at a frequency specified in the internal regulations. In this respect, the MNB regards it as good practice to perform the review at least annually and in the case of all significant changes affecting the financial institution or group (e.g. change in the external environment, establishment of a new subsidiary, selling any of the group members, acquisition) to perform an extraordinary review in a documented manner and to modify the structure as necessary in due course.
23. According to the MNB's expectations, it is the responsibility of the financial institution's governing body to review the financial institution's policies as necessitated by the new organisational structures and, if necessary, to develop new policies.

IV.2.2 Complex structures, non-standard or non-transparent activities

24. The financial institution is expected to develop a transparent organisational framework and operational structure. The MNB regards organisational structures that are not justified by economic or legal objectives, that are vague or unreasonably complex, that are incomprehensible to employees and authorities, or that facilitate the commission of criminal offences (e.g. money laundering, terrorist financing, fraud) affecting the financial intermediary system, or operational practices that deviate from the established organisational structure as unacceptable.

25. The following practices call for the special attention of both the financial institution and the MNB:
- a) the development of complex, but justifiable, organisational frameworks and operational structures, including, for example, the provision of services through a special purpose vehicle or similar arrangement;
 - b) the provision of services or products deviating from the usual standards or not transparent to the financial institution or the customers; and
 - c) activities in countries the financial regulatory practices of which substantially differ from the international and Hungarian standards, recommendations or regulation.
26. The MNB expects the financial institution or group to pursue the practices under point 25 only with due foresight and on the basis of a thoroughly considered strategy and policy, approved and regularly reviewed (with the frequency and in the manner specified in its internal regulations, in respect of which the MNB regards annual review as good practice) by the financial institution's governing body.
27. In the cases under point 25, the MNB also expects the following to be enforced:
- a) the management of the financial institution should understand the purpose of the applied practice;
 - b) the associated risks are identified before the practice is applied and the management of the financial institution should understand the extent and nature of those;
 - c) the financial institution should have policies and procedures in place to monitor, mitigate, control and report the arising risks (including the provision of information to the governing body, the areas in charge of internal control functions and the oversight function, the external auditor and the MNB) consistent with the risks of the practice;
 - d) the areas with internal control functions in the financial institution should pay special attention to the applied practices;
 - e) the financial institution should regularly assess the justification for maintaining the practice;
 - f) the decision on the applied practice, the findings of the area in charge of internal control¹⁰ in relation to the applied practice, and the assessments related to the maintenance of the applied practice should be documented.
28. The MNB expects financial institutions to treat the complex organisational frameworks and operational structures used by their clients also with due foresight and to enforce the corporate governance principles under this recommendation also in the case of non-standard and non-transparent activities carried out on behalf of clients.

¹⁰ Although a specific internal control function may be performed by a single person, a single organisational unit or by several persons, organisational units or areas, the recommendation always refers to those exercising the function as the area performing the respective function.

IV.2.3. Prevention of money laundering and terrorist financing

29. The MNB expects the financial institution or group to establish and operate appropriate processes and procedures in order to fulfil its obligations related to the prevention of money laundering and terrorist financing. As part of this, the financial institution is expected to assess regularly the financial institution's or group's exposure to money laundering and terrorist financing risks and, where necessary, take measures to reduce or eliminate these and other risks (such as reputational and operational risks) associated with money laundering and terrorist financing risks, including the training of employees on money laundering and terrorist financing risks.
30. In connection with the prevention of and combating money laundering and terrorist financing, the MNB expects, in addition to the application of Article 63(5) of the AML Act, that a member of the financial institution's governing body is designated – duly considering potential conflicts of interest – as responsible for compliance with the requirements and expectations related to the prevention of and combating money laundering and terrorist financing. If the financial institution has no governing body, a member of the senior management of the financial institution is expected to be designated as responsible for compliance with the requirements and expectations relating to the prevention of and combating money laundering and terrorist financing. The appointment of a member in accordance with the foregoing shall not prejudice other duties and responsibilities of the management body or senior management in relation to the management and activities of the financial institution or group.¹¹

IV.2.4 Group level organisational frameworks

31. In the case of the controlling financial institution the MNB expects its management to know the reason for and the purpose of establishing or acquiring the individual subsidiaries and other group members, the operating risks related to the entire group, intra-group transactions as well as the funding, capital and risk profile consequences of group-level operations under normal business conditions and in crisis situations.
32. In the case of the controlling financial institution, the MNB also expects it to establish an efficient and transparent group structure and group-level operational structure to ensure that the relationships and transactions between group members, whether domiciled in a third country or in an offshore financial centre, do not compromise the implementation of the requirements under points 5 to 9 of the recommendation regarding the establishment and operation of internal lines of defence at group level.

¹¹ MNB Recommendation No 7/2019 (IV. 1.) – at the time when this recommendation is issued – on assessing the risk of money laundering and terrorist financing associated with financial institutions and on determining related measures, also specifies additional requirements for credit institutions defined in Article 3(16) and for financial service provider defined in Article 3 (28) of the AML Act.

33. The MNB expects the governing body of the controlling financial institution to ensure that group members have access to sufficient information about the entire group's overall objectives, strategies and risk profile, and to understand how the group members fit into the structure and functioning of the group. The relevant transfer of information shall be documented by the financial institution and made available to the body or area (including the executive board, business lines and internal control functions) in charge of the respective function.
34. The governing body of the controlling financial institution shall be regularly informed of the risks inherent in the group's composition and operational structure, in respect of which the MNB regards it as good practice to perform the assessment at least annually.

IV.3. Monitoring system

35. The MNB expects the governing body of the financial institution or group – duly considering the principle of proportionality outlined in point 10 – to develop and operate a monitoring system and audit trail for the activities of the financial institution or group, documented in internal regulations. The audit trail shall include in particular the levels of responsibility and information and the links between the individual activities as well as the management and monitoring processes, facilitating the tracking and subsequent control of those. The audit trail shows the weaknesses in the organisation's control system and helps identify risks. The audit trail is designed to make in-process, preliminary and subsequent management controls as well as independent internal and external audits more effective. To this end, it is recommended that audit trails should include the identification of the processes or activities available in the financial institution, the designation of the job or role responsible for management of those, the legal basis (law, internal regulations) of the performance of the processes or activities, and a more detailed description of the tasks related to the process or activity element. Those should also include the title of the main types of documents and databases related to the latter task description, the deadline for the completion of the process or activity, the description of the risk(s) (broken down by relevant risk), the control point related to the performance of the process or activity and the homogeneous single risk(s), the designation of the job or role of the person performing the control, in a manner that facilitates, based on the job description, a clear identification of the person performing the control and the frequency of the control.

IV.3.1 In-process monitoring

36. The financial institution is expected to design the individual business processes and internal rules in a way that facilitates in-process monitoring. The financial institution is expected to include checkpoints in each process to ensure that each sub-task can only be performed after the verification of the previous sub-task – including the adequacy thereof – thereby ensuring the adequacy of the inputs of the sub-tasks built on each other. The same person should not

be responsible for performance, processing and monitoring of a specific operation (appropriate level of segregation of duties/four eyes principle). The job descriptions shall include the obligations to comply with the monitoring tasks integrated in the workflow defined in the internal administration regulations. The financial institution shall develop its procedures in such a way that all transactions involving a risk can be executed only after a documented control based on the four eyes principle or an automated verification that includes pre-defined controls.

37. The MNB recommends to the financial institution that it should develop dual reporting paths in the business areas and that reporting on positions and risks should also reach the risk management function in addition to senior managers of the business lines.

IV.3.2 Management control

38. The purpose of creating different management levels and of the organisational structure is to achieve the goals and the strategy of the financial institution or group more efficiently. The management control functions and responsibilities are expected to be enforced at all management levels. The purpose of the management control is to check, among other things, the proper operation of the in-process control points. The tools of management control include reporting, request for reports, exercising the right to sign, checking the content, form and other aspects of the performance of tasks, personal on-site inspections and the operation of the management information system. The managers of the financial institution regularly monitor and order their subordinates to give account of their work in line with the provisions of the internal policies and procedures. The detailed rules for management control (including reports and reporting lines) are described in full in the internal regulations.

IV.3.3 Management Information System

39. The development and operation of a management information system covering the full range of activities is an important element of the financial institution's operation. The purpose of the management information system is to provide the management with consistent and comprehensive information in a timely manner for management and control purposes.
40. The management information system of a financial institution comprises all information (at the level of the financial institution and group) received for the management, and the system that collects and processes the information and delivers it to the target persons in a way that ensures that the manager can react to changes in a timely manner.
41. The MNB recommends to financial institutions to use primarily electronic tools and channels for the operation of management information systems.

42. The management information system is expected to be designed and operated in a way that supports the management of the financial institution or group with reliable and relevant information available in a timely manner.
43. In addition, the information systems are expected to be secure, audited independently and regularly and prepared for unexpected events.

IV.4 Corporate system, governance and supervisory functions

44. The MNB expects the financial institutions to operate, in compliance with the legal requirements, corporate systems that ensure the efficient and prudent exercise of governance and supervisory functions within the financial institution or group. In the Hungarian corporate governance practice, partly due to the different legal background, there are differences between the different types of financial institutions and also within the individual sectors.¹² Accordingly, the MNB does not consider the formal existence of these bodies alone to be sufficient, but it rather expects the implementation and efficient operation of the management and supervision functions, as well as the clarity and transparency of the applied practice.
45. The financial institution is expected to specify in writing (e.g. in a Memorandum of Association, OOR, rules of procedure, internal regulations) its bodies performing the main management and supervision functions, their duties and powers, and the main rules of procedure governing their activities, duly considering the statutory requirements.
46. In connection with the requirement under point 45, the role of the different bodies (management, board, executive board, board of directors, supervisory board, audit committee) in the financial institution or group, based on the applied division of tasks and responsibilities
 - a) in the definition of the business and operational objectives of the financial institution, in the development and implementation of its strategy in compliance with the effective statutory requirements and considering the owners' economic and social objectives,
 - b) in the definition of risk appetite and in the elaboration of the risk strategy and policies facilitating the achievement of the objectives resulting from those, including the allocation of capital to cover risks and the definition of liquidity management objectives,
 - c) in the creation and maintenance of a corporate culture and risk assumption satisfying the expectations of the recommendation, and a risk culture that covers all aspects of risk management and risk control as well as in the development and operation of a risk management framework,

¹² Many financial institutions operate separate management, boards of directors and supervisory boards as the main governance and controlling bodies. At others the composition of the executive and management board is identical, and there are also some models where no separate executive board exists.

- d) in the communication of objectives and policies – including also the transmission of corporate governance principles and corporate values – within the organisation and the group as well as in the outward communication of those (to the markets and authorities),
- e) in the elaboration and approval of related internal regulations and guidelines as well as in providing the conditions and resources necessary for the application of those,
- f) in the establishment of an effective governance system for the financial institution or group, including a transparent organisational structure and committee system, supplemented with appropriate communication and reporting channels,
- g) in the definition and application of policies and procedures for the selection, nomination, appointment and succession of the chairperson and members of the board of the financial institution or group, and of key management personnel as well as in the definition and application of remuneration policies,
- h) in the management of conflicts of interests
- i) in the verification of the compliance of operations with the strategy and policies,
- j) in reviewing and, where necessary, amending the strategy and policies at regular intervals – where the MNB regards it as good practice to review policies at least annually – with the frequency and in the manner laid down in internal regulations,
- k) in developing, harmonising and maintaining strong internal control functions,
- l) in establishing and operating processes for accounting reporting, disclosure and supervisory reporting and ensuring their integrity,
- m) in overseeing other contacts and communication with external stakeholders,
- n) in the regular – at least annual – evaluation of the functioning of the management system and internal lines of defence of the financial institution or group as well as of the elements constituting its sub-areas, considering both internal and external changes, and in taking the necessary corrective measures shall be also laid down in writing

47. The key duty of the governing body is the practical implementation of the strategy of the financial institution or group.

48. The key duty of the supervisory bodies is to monitor and oversee the practical implementation of the strategy. The sectoral legislation specifies the mandatory tasks of the supervisory bodies with a narrower scope, typically focusing on the tasks related to the preparation of the financial statements and the management of the internal audit organisation.¹³

49. In connection with the statutory tasks of the bodies in charge of supervisory functions¹⁴ it is recommended to obtain the prior consent of the body fulfilling supervisory functions for decisions related to the establishment and termination of the employment relationship and remuneration of the head of the internal audit organisation, chief internal auditors and the

¹³ See Section 152(3) and (5) of the Credit Institutions Act and Section 85(4) of the Insurance Act

¹⁴ This is a statutory requirement for financial institutions falling within the Credit Institution Act and the Insurance Act.

internal auditor discharging his duties on his own as well as, in line with sub-point f) of point 108, for the dismissal of the head of the risk control and quality assurance functions.

This expectation does not cover all staff members of the internal control area, only those in charge of managing the area, and does not affect the responsibility of the internal control function or the rights of the employer over the persons performing the activities of that internal control function.

50. The MNB regards it as good practice for a financial institution's supervisory body to pay attention to the following activities in addition to its key statutory tasks:
- a) monitoring the decision-making activities and supervision of the governing body,
 - b) critical evaluation of the decisions of the governing body and of the information provided by that body,
 - c) monitoring and regularly evaluating the functioning of the internal lines of defence of the financial institution or group – in this respect, the MNB regards it as good practice to carry out evaluations at least once a year – and to initiate the necessary measures if any shortcomings are detected,
 - d) monitoring and supervising the strategic objectives, organisational structure, risk strategy – including the risk appetite and the risk management system – and disclosure practices of the financial institution or group,
 - e) monitoring developments in the risk culture of the financial institution or group,
 - f) overseeing compliance with the financial institution's or group's ethical norms and measures to manage conflicts of interest,
 - g) overseeing the integrity of the compilation of financial statements and supervisory data supply.
51. The MNB is of the opinion that it is appropriate for the supervisory board of a financial institution or group to obtain information on the functioning of internal lines of defence not only from the reports received from the governing body, but also to maintain direct contact with the internal control function. In this respect, it is recommended that a summary assessment is prepared at least annually¹⁵ by the head of the compliance area, the head of the risk control function and the internal auditor¹⁶ for the bodies with the oversight function and it is discussed by the board. If the financial institution has an audit committee, the board with supervisory function may also perform the aforementioned tasks through that.
52. The members of a financial institution's or group's supervisory bodies – even if not necessarily each of them, or not in all cases or on all topics
– are collectively willing and able to

¹⁵ For internal audit the Credit Institutions Act and the Insurance Act prescribe half-yearly and quarterly reporting obligation, respectively.

¹⁶ The statutory requirements do not prescribe a complex overview, but rather focus on a single element of the internal lines of defence. Usually, the internal audit area has a reporting obligation to the supervisory board.

- a) understand and evaluate the proposals and explanations formulated and information provided by the body exercising the governance function in the financial institution or group,
 - b) monitor the application of its strategy, risk appetite and policies,
 - c) to evaluate the performance of the persons with functions in its governing body.
53. The MNB expects the governing and supervisory bodies of the financial institution or group to cooperate with each other efficiently, through sharing information to the necessary and adequate degree. To this end, the body exercising the governance function of the financial institution or group (e.g. the board of directors) shall regularly – with the frequency and in the manner specified in the internal regulations – discuss the business and risk strategy of the financial institution or group and the implementation of those with the bodies exercising the supervisory function of the financial institution or group (e.g. the supervisory board), and shall promptly inform the latter of any external and internal events, processes and trends affecting the governance and safe operation of the financial institution or group.
54. The chairman of the supervisory body is expected to send to the MNB – within ten days of the committee meeting – the minutes, proposals and reports relating to the agenda item discussed by the supervisory body on serious breaches of the internal rules of the financial institution or serious irregularities in management or governance.¹⁷

IV.5 Expectations towards board members

55. The MNB expects the financial institution to exercise due diligence in selecting, assessing the suitability, evaluating the performance, and planning the succession and reappointment or election of the chairpersons and members of the boards with governance and supervisory functions, or their assignment to other positions within the organisation. In this context, the MNB also considers it appropriate for larger, more complex financial institutions to operate a nomination committee¹⁸, the tasks of which include in particular:
- a) nominating and recommending candidates for board membership, taking into consideration the relevant legal requirements (in particular with regard to the number of members in the individual bodies, the ratio of external and internal members, the independence of members and compliance with the requirements related to gender representation) and the related supervisory regulatory tools;
 - b) identifying the skills and responsibilities required for the particular board membership and assess the time needed to carry out those responsibilities;
 - c) assessing the individual and collective suitability of board members;

¹⁷ In the case of financial institutions falling within the Credit Institutions Act [Article 152 (6)], this is also a statutory requirement for the executive body with supervisory powers, while based on Article 272 of the Insurance Act it is the duty of the chairman of the supervisory board.

¹⁸ The establishment of a nominating committee pursuant to Article 112(1) of the Credit Institutions Act is also a statutory requirement for credit institutions with a market share of at least five percent based on balance sheet total, and pursuant to Article 24/D(1) of the Investment Firms Act for investment firms with a balance sheet total exceeding HUF 200 billion.

- d) assessing the size, composition and performance of the boards at least once a year and formulating a recommendation to address any shortcomings, including measures to be taken upon breaching the statutory limits;
- e) regularly reviewing the policy for the selection and appointment of the chief executive of the financial institution and, on the basis of the findings, making recommendations to the body with governance function;
- f) regular review whether the board decisions are free from influence.

56. In terms of defining the number and composition of the bodies with governance and supervisory function, and selection and performance assessment, the financial institution is expected to act in accordance with an appropriate internal policy, which lays down the necessary professional and qualification requirements, skills and experience. In the course of the foregoing, the financial institution is expected to take into consideration the business model of the financial institution or group, the special features, scope, complexity and risks of the service activities pursued by it, in addition to the statutory requirements and the expectations specified in the related supervisory regulatory instruments, in particular in MNB Recommendation No 1/2022 (I.17.).

57. The following aspects should be considered in the course of the selection and succession planning process:

- a) the necessary qualifications, skills and competences of the chairperson and of each member of the boards should be defined in such a way as to ensure that the appropriate expertise, skills and experience are available for the board as a whole;
- b) where it is possible for the same person to be a member in several boards, hold more than one position or be responsible for a control function, the different functions should not represent a conflict of interest and the negative effects of this should be minimised (for example, overburdening should not prevent the person from performing each position to a high standard);
- c) the suitability of the candidate should be assessed even at those financial institutions and in respect of those positions where this is not specifically stipulated as a statutory licensing condition or other requirement; in this respect the MNB regards it as good practice to take into consideration the requirements of MNB Recommendation No 1/2022 (I. 17.);
- d) even under a different – permissive – statutory requirement, the financial institution should strive to ensure that the mandate of a member is not open-ended and that, in the case of a fixed-term mandate, the member is only reappointed if the financial institution has duly assessed the member's activities in the preceding period and it found that he had duly performed his duties in line with expectations;
- e) the expiry of the mandate of several members at the same time may constitute an operational risk, which should be addressed by the financial institution.

58. The members of the governing and supervisory bodies are expected

- a) to proceed actively with the highest professionalism and due diligence;
- b) to be able to make independent, objective and informed decisions, to take action and express their opinions;
- c) to be able to devote sufficient time to their functions, also considering their other duties and responsibilities.

59. With regard to the independence of the board members, the general rules of Act V of 2013 on the Civil Code (hereinafter: Civil Code) shall apply, also taking into consideration the requirements of the legislation applicable to the sector. In addition, the MNB proposes that the financial institution should apply the requirements of independence applicable to the members of the board of directors under Article 3:287 of the Civil Code to the widest possible range of the members of the supervisory bodies.

60. The provisions of the Civil Code and sectoral legislations shall be followed also with regard to the professional qualifications of the bodies with supervisory function. On the other hand, continuous enhancement of expertise, skills and competencies is essential for continuous compliance. To this end, as a good practice, the financial institution shall provide or make available training programmes to board members, tailored to the needs of the financial institution or group, with appropriate time, budget and resources.

IV.6 Operation of the boards

61. As regards the operation of the governing body, it is expected to have a set of rules in place guaranteeing the active participation of all members and the possibility of expressing their professional position (for example, by specifying in the statutes of the body the schedule of meetings and the possibility of making comments). The MNB considers it important for the efficient operation of the financial institution that its bodies with governance and supervisory functions have regular meetings and conduct their activities in accordance with the rules of procedure, which specify, in particular, the frequency and manner of convening and holding meetings, the procedures for determining the agenda, the preparation and approval of minutes, the required attendance and voting ratios for certain decisions, and the rules of reporting, in compliance with the statutory requirements. In this context, the MNB expects the governing and supervisory bodies of the financial institution to carry out their work based on decision-supporting documents of adequate volume and quality and that sufficient time is allowed for taking decisions. It is also expected that the minutes of the board meetings and the documents related to decisions taken outside the meeting describe the meeting with a level of details that allows a third party to reconstruct the relevant circumstances of the decision (the material aspects considered, the main arguments and counter-arguments, essential comments, the aspects underlying the proposed decision, the voting ratios, the content of the substantive decisions).

62. The chairman has a key role in the operation of the boards, who is expected by the MNB to
- a) contribute to the establishment of a transparent system of responsibility within the board;
 - b) ensure the continuous operation of the board;
 - c) foster effective communication and cooperation of sufficient degree within the board and with other bodies and committees, and with the exercisers of other functions;
 - d) make efforts to ensure balanced decision-making based on open, professionally informed disputes, with sufficiently critical attitude, and ensure that individual positions, departing from the majority, are recorded, in order to ensure the effectiveness of the internal lines of defence.
63. The MNB expects that the work of the financial institution's governing and supervisory bodies is regularly assessed by the superior body at a frequency and in a manner specified in the internal regulations. An external person may also be involved in this.

IV.7 Committees

64. The work of the financial institutions' bodies with governance and supervisory functions is also assisted by several committees to be established based on statutory provisions and operated in accordance with the relevant requirements (e.g. composition, membership requirements) (e.g. audit committee in the case of a credit institutions, investment firms, insurance or reinsurance companies of public interests, or underwriting and risk management committee, nomination committee and remuneration committee in the case of credit institutions with a market share of at least five percent based on balance sheet total).
65. Pursuant to the provisions of Article 3:291 of the Civil Code and the special requirements of the laws applicable to the sector (with special regard to the requirements concerning the composition and tasks of the committee) credit institutions, investment firms, insurance and reinsurance companies of public interest shall set up and operate an audit committee, which shall support the financial institution's¹⁹ supervisory body in the inspection of the financial reporting system, in the selection of the auditor and in the cooperation with the auditor. The MNB supports the efforts of financial institutions to set up audit committees also in cases not designated by the statutory provisions, considering their special features.
66. The tasks of the audit committee established at the financial institution's own initiative should be defined considering the tasks of the supervisory body, taking into account the tasks defined for the supervisory body and the audit committee in this recommendation and based on the statutory provisions. In the case of an audit committee established at the financial institution's own initiative, the MNB regards it as good practice for an audit committee to perform the following tasks:

¹⁹ Section 157 of the Credit Institutions Act, Section 20/C of the Investment Services Act, Section 116 and 117 of the Insurance Act

- a) monitoring the functioning of internal lines of defence in connection with the preparation of the financial statements,
- b) overseeing the formulation of accounting policies,
- c) monitoring the process of compiling financial statements and formulating recommendations as necessary,
- d) verifying compliance with the legal requirements concerning the independence of the external auditor,
- e) monitoring the statutory audit of the annual and consolidated financial statements,
- f) as regards the selection of the auditor, also considering the provisions of point 172, proposing an auditor for the appropriate body of the financial institution,
- g) assessing the scope of the statutory audit of the annual and consolidated financial statements,
- h) reporting the results of the audit to the appropriate body of the financial institution and interpreting the results,
- i) receiving and evaluating additional audit reports.

67. In order to ensure the effective operation of the internal lines of defence, it may be also appropriate to establish committees that are not prescribed by law (for example, an audit committee, underwriting and risk management committee, nomination committee or remuneration committee at a financial institution that is not required to have one, or a compliance committee, HR committee, ethics committee, money laundering and terrorist financing prevention committee at all financial institutions), in accordance with the nature of the financial institution's business model, the special features, scope, complexity and risks of the service activities carried out by the financial institution or group, and the role of the financial institution in the financial intermediary system).

68. Of the committees to be established based on statutory regulations, credit institutions with a market share of less than five percent based on balance sheet total may combine the underwriting and risk management committee with the audit committee²⁰. In this case, the credit institution is expected to act with due care when combining its committee to be established based on statutory provision, with other committees, considering the need to manage any potential conflicts of interest that may arise. However, the MNB regards due care as a fundamental principle for all committees of the financial institution when combining the committees.

69. The established committees are expected to operate with a clear and documented division of powers and responsibilities, ensuring access to all relevant information and data²¹ and other necessary resources for the tasks to be performed.

²⁰ Section 157(4) of the Credit Institutions Act

²¹ The range of relevant information and data may vary depending on the activities of each committee, but may also cover legal, financial, HR and IT data as well as data and information generated within the framework of the operation of the risk control, compliance or internal audit function

70. The MNB does not regard it as good practice to set up and operate the different committees with a fully identical composition. However, subject to exercising due care, ensuring the management of conflicts of interest and preserving the independence of the original function, with a view to enhancing the efficiency of the cooperation between committees it may be useful in certain cases if the same persons participate in several committees simultaneously (e.g. compliance committee - ethics committee, AML/CFT committee or risk management committee - compliance committee) and the members are rotated.
71. The MNB also expects committees to ensure the availability of appropriate expertise, competence and experience for the committee as a whole, and to give priority to the principle of diversification (gender, age, professional experience, competences) in the composition of committees.
72. In the case of credit institutions, investment firms, insurance or reinsurance companies of public interest, it is good practice if at least one member of the audit committee or other body performing those functions based on a statutory mandate also holds an auditor qualification.²²
73. As regards the auditing qualifications of the members of the audit committee or any other body performing its duties on the basis of a statutory authorisation, the MNB considers it as good practice if the auditor member also holds a qualification under Article 49/A a)-d) of Act LXXV of 2007 on the Chamber of Hungarian Auditors, the Activities of Auditors, and on the Public Oversight of Auditors (hereinafter: Auditor Act) relevant for the respective financial institution (financial institutions, investment firm, fund, insurance company). It is also good practice for a financial institution applying international financial reporting standards if the auditor member also holds an IFRS qualification under Article 49/A (f) of the Auditor Act.
74. Compliance with the general requirements concerning the operations of the boards, outlined in Articles 61–63, is recommended also in respect of the operation of the committees.

IV.8 Standards applicable to the operation of the financial institution

75. The MNB expects the management of a financial institution to establish high ethical standards and internal professional standards aimed at mitigating risks, tailored to the needs and characteristics of the financial institution or group and its role in the financial intermediation system.

(including information related to compliance with requirements and expectations related to the prevention of money laundering and terrorist financing).

²² Pursuant to Article 3:291(2) of the Civil Code and Article 116(3) of the Insurance Act, the existence of accounting and auditing qualifications is an alternative condition.

76. It is appropriate to realise the application of ethical and professional standards within the financial institution or group through policies adopted by the financial institution's governing body, which stipulate
- a) that the financial institution conducts its activities in accordance with the applicable laws and accepted corporate values,
 - b) the financial institution fosters risk awareness by creating and maintaining a strong risk culture – also supported by the remuneration policy – and communicates the expectation of the financial institution's management according to which the activities should be conducted in accordance with the risk appetite and limits set by the financial institution and the responsibilities of individual staff members,
 - c) acceptable and unacceptable behaviour (supported by examples),
 - d) in addition to complying with legal requirements and internal policies, the employees are expected to act honestly and fairly and to carry out their duties with due professional skills, care and diligence,
 - e) the possible internal and external measures and sanctions in the event of breach of duty and unacceptable behaviour.
77. The financial institution is expected to ensure that its employees are not discriminated on the grounds of sex, race, mother tongue, colour, ethnic or social origin, genetic characteristics, religious or other beliefs, national minority status, property, birth, marital status, health, disability, geographical location, age or sexual orientation and to provide all employees of the financial institution with equal opportunities and gender-neutral treatment (in particular with regard to recruitment, remuneration, career development and succession opportunities, return to work after long-term absence and access to training), and furthermore, the financial institution should make efforts to improve the representation of underrepresented genders within management bodies and across all categories of employees whose professional activities have a material impact on the risks of the financial institution.
78. The MNB expects the financial institution to ensure that the employees of the financial institution are familiar with and apply in practice the relevant ethical norms and professional standards. The MNB expects the financial institution to lay down in its internal regulations which area or areas of the internal control function are responsible for monitoring compliance with ethical norms and professional standards, investigating breaches of ethical norms and professional standards, and reporting on compliance with ethical and professional standards to the body with governance function.

IV.9 Management of conflicts of interests IV.9.1 Conflicts of interest at organisational level

79. The financial institution or group should have a policy, adopted and regularly reviewed by the body with governance function, related to the identification, assessment and management of conflicts of interest that may prejudice the interests of clients arising from an activity of a member of the financial institution or financial group.

80. The policy related to the management of conflicts of interest across the organisation is expected to identify relationships, services, activities or transactions that may give rise to a conflict of interest and specify potential methods, procedures, responsibilities and timelines for addressing those.
81. The tools for managing conflicts of interest at organisational level, include in particular:
- a) appropriate segregation of duties and responsibilities in internal regulations with sufficient level of details (for example, by allocating monitoring and reporting responsibilities to different persons in the case of activities involving conflicts of interest),
 - b) development of information barriers (e.g. through physical separation),
 - c) developing procedures for transactions with external parties, where it is good practice to define the different operational approval levels and the involvement of the compliance area in the approval process without taking final responsibility for the decision.

IV.9.2 Conflicts of interest at personal level

82. The financial institution or group should have a policy related to the management of conflicts between the interests of the financial institution or group and the different interests of the employees of the financial institution or group members, adopted and regularly reviewed by the body with governance function²³; such policy may also form part of the policy under point 79 or of other internal regulations, subject to point 13.
83. The MNB expects the policy for identifying, assessing and managing conflicts of interest at individual level to cover the following situations and relationships that may (but do not necessarily) give rise to a conflict of interest:
- a) economic interests (e.g. shares, other ownership rights and memberships, financial investments and other economic interests in trading partners, intellectual property rights, loans granted by a financial institution to a company owned or controlled by an employee or a close relative of an employee, membership in or ownership of a body or organisation with conflicting interests),
 - b) a personal (e.g. family) or professional relationship with an owner holding a controlling interest in a financial institution or in a member of the financial group,
 - c) a personal (e.g. family) or professional relationship with an employee of the financial institution or a member of the financial group,
 - d) other employment relationship and recent previous employment, particularly in the last five years,

²³ This is usually regarded as a conflict of interest policy.

- e) any personal (e.g. family) or professional relationship with relevant external parties (e.g. significant suppliers, auditors, consultants or other service providers, including entities buying the financial institution's receivables),
- f) political influence or political relations.

84. The financial institution or group is expected to lay down the following criteria in its internal rules on the management of conflicts of interest at personal level:

- a) the criteria for identifying potential conflicts of interest at personal level (types of situations and relationships that may give rise to a conflict of interest, assessed by the financial institution),
- b) the timeframe for identifying potential conflicts of interest at personal level (how far back in time it is necessary to examine the situations and relationships that constitute a potential conflict of interest, also considering the relevant data protection requirements),
- c) the cases of conflicts of interest at personal level deemed significant (with an itemised list in addition to qualitative criteria),
- d) provisions related to the identification, assessment, ongoing monitoring and control of internal systems, procedures and methods applied to identify, assess, monitor and control conflicts of interest at personal level, including the reporting of situations and relationships representing potential conflicts of interest, and to the regular review of those, including in particular, laying down the requirement to make a declaration of conflict of interest at least every two years and the obligation to report any change in the information provided,
- e) designation of the person, organisational unit or function with primary responsibility for identifying, assessing and monitoring conflicts of interest at personal level,
- f) roles, responsibilities and powers relating to the identification, assessment, ongoing monitoring and management of conflicts of interest at personal level, in particular the tasks of persons involved in a potential conflict of interest as well as of the person, organisational unit or function referred to in subpoint e) and of the internal control functions,
- g) means of managing conflicts of interest at personal level, distinguishing between the means of mitigating or eliminating risks arising from persistently existing potential conflicts of interest and considered significant by the financial institution, and the means of managing one-off situations (for example, entering into a single transaction with an external supplier),
- h) documentation and record-keeping requirements related to the identification, assessment, continuous monitoring of conflicts of interest at personal level and to the measures taken, ensuring the comprehensive and up-to-date registration of those.

85. The MNB expects the financial institution to act with special care when managing conflicts of interest arising in respect of the members, key management personnel, auditors and immediate family members of bodies in charge of governing or supervising the financial

institution and the group members. The range of people in key positions may vary by sectors and by financial institutions. In line with MNB Recommendation No 1/2022 (I. 17.), the MNB regards it as good practice for the financial institution to treat the managers of branches and subsidiaries in other Members States and in third countries, the managers of key business and supporting areas (e.g. head of treasury, head of investments, head of IT), the head of the internal control functions, – if relevant – the manager under point 101 and the heads of other areas with special controls functions and duties, under point 110, as well as the non-executive persons subject to special remuneration, as persons filling key positions; other persons may also be classified as persons with significant influence on the operation of the financial institution.

86. The tools for managing conflicts of interest at personal level, may include in particular:

- a) regular training and awareness-raising campaigns on situations, practices and transactions that give rise to conflicts of interest, including regular calls for the completion of conflict of interest declarations, specified in the internal regulations;
- b) allocation of activities or transactions giving rise to a conflict of interest²⁴ to different persons;
- c) prescribing the obligation to report situations, practices and transactions that give rise to a conflict of interest;
- d) comprehensive and retrievable recording and registration of conflicts of interest declarations with negative clearance, and the content of notifications related to situations, practices and transactions giving rise to a conflict of interest, and keeping the registers up-to-date;
- e) verifying the content of declarations and notifications under subpoint d), subject to the principle of proportionality;
- f) restricting situations, practices and transactions that give rise to a conflict of interest, as a whole or over a specific limit;
- g) prescribing the avoidance of situations, practices, transactions other than those involving an approved conflict of interest;
- h) preventing employees active outside the financial institution (for example, through other working relationships with other organisations) from gaining undue influence in the financial institution through their activities outside the financial institution;
- i) development of a specific decision-making practice on risk assumption concerning transactions involving a conflict of interest: in connection with this the MNB expects the financial institution during the preparation of the decision to assess in detail the impacts of such risk assumption on the risks of the financial institution, to prescribe the application of arm's length conditions and that the risks assumption is decided by an executive body or committee; however, depending on the magnitude of the transactions and their impact on the financial institution's risk, practices departing from the foregoing may also be

²⁴ For the purposes of points 86 and 87, all legal relationships resulting in an exposure shall be considered as transactions.

applied (e.g. in the case of transactions resulting in small exposures, below the limit stipulated in the internal regulation, the application of conditions more favourable than the market conditions, may also be acceptable); on the other hand, the financial institution is expected to specify in its internal regulation the range of transactions (e.g. based on volume, product type or contractual conditions) in respect of which the decision by the executive body or committee must not be waived; the MNB is of the opinion that transactions concluded subject to special conditions better than the market conditions, resulting in a conflict of interest, must be regarded as such transactions in all cases;

- j) requiring members of boards with governance and supervisory functions to abstain from voting on any matter where the respective member has or may have a conflict of interest or where the member's objectivity or ability to properly discharge his duties to the financial institution may be compromised;
- k) with the exception of positions filled in the institutions falling within the institution protection scheme mentioned in Article 113(7) of CRR, in credit institutions permanently affiliated to a central organisation mentioned in Article 10 of CRR, and in an another member of financial group that also includes the respective financial institution, to prevent the member of the executive body from holding a position in the board of directors of another financial institution.

87. In connection with the application of the requirement specified in subpoint d) of point 86, in respect of the transactions concluded with a member of the credit institution's executive body, with an undertaking in which a close relative of a member of the executive body has a controlling interest and with undertakings where the member of the executive board or close relative of the member of the executive board is a senior executive as specified by the Civil Code, with a view to ensuring the statutory record-keeping,²⁵ the MNB prescribes the documentation of the following information:

- a) information that facilitate the identification of persons participating in the transaction,
- b) type/nature and amount of the transaction and the applicable terms and conditions,
- c) the date when the transaction was approved and the name of the person, body or committee that decided on the approval, information on whether or not the transaction was at arm's length terms and, if not, whether or not the transaction was at terms available to all employees, and
- d) if the transaction amount exceeds EUR 200,000, the following supplementary information:
 - da) the ratio of the amount of the exposure to the sum of core capital and Tier 2 capital and to the Tier 1 capital,
 - db) the ratio of the sum of the exposures to the same debtor to the sum of core capital and Tier 2 capital and to the Tier 1 capital,
 - dc) whether the exposure qualifies as a large exposure, and dd) the ratio of the amount of exposures to the same debtor to the total exposures that the financial institution has undertaken vis-a-vis the member of its executive body, an undertaking in which a close

²⁵ Section 144(6) of the Credit Institutions Act

relative of a member of its executive body has controlling interest or an undertaking in which the member of its executive body or the close relative of a member of its executive body is a senior executive as specified in the Civil Code.

88. The MNB expects investment firms not applying the provisions of CRR and not qualifying as a small and unrelated investment firm to apply subpoints a)-c) of point 87.

IV.10 Management of risks

IV.10.1 Risk awareness

89. Risk forms an integral part of the activities of financial institutions, in the management of which a risk culture supporting prudent, consistent and substantiated decision has a key role. Accordingly, financial institutions are expected to develop an integrated risk culture encompassing the entire institution and/or the group and their all risks,

which ensures the identification, assessment and management of the arising risks in accordance with the risk appetite and risk tolerance level of the institution and/or the group. When developing their risk management culture, the MNB expects investment firms not applying the provisions of CRR and not qualifying as small and unrelated investment firms to take into consideration the risks affecting clients, markets and the investment firm as well as liquidity risks, particularly those that may have a significant impact on the level of available own funds or may exhaust those.

90. The primary means of creating a risk culture include internal policies, regulations, guidelines, communication, training of employees in line with their responsibilities in risk assumption and risk management, and the activities, strategy and risk profile of the financial institution or group.
91. Elements of a strong risk culture include, among other things:
- a) top-down scale of values: the body with the governance function is responsible for establishing the core values and expectations of the financial institution or group, communicating them to the employees, monitoring and evaluating the risk culture and initiating changes to the risk culture as necessary,
 - b) accountability: employees are aware of the risk appetite and risk capacity of the financial institution or group to the extent that is proportionate with their responsibilities, they perform their work with due regard to these, and are responsible for complying with the limits broken down to the level of individual employees,
 - c) effective communication and critical attitude: a prudent risk culture fosters open communication, the consideration of differing opinions in decision-making, encourages

constructive criticism from employees and creates an open and constructive participative environment for the organisation as a whole,

- d) incentives: appropriate incentives play a key role in aligning the risk-taking behaviour with the risk profile and long-term interests of the financial institution.

92. In order to enable a financial institution to make informed decisions based on the identification, measurement or assessment and monitoring of risks, the MNB considers it necessary to implement a comprehensive approach to risk management practices that

- a) covers the financial institution or group as a whole, all of its members, organisational units business areas and activities, including outsourced activities,
- b) recognises the economic substance and risks of activities and exposures,
- c) addresses all relevant risks, such as credit, market, operational, liquidity, insurance, reinsurance, concentration, strategic, actuarial, reputational, compliance risks as well as money laundering, terrorist financing, climate change, environmental, social and governance risks,
- d) facilitates the bottom-up and top-down aggregation and decomposition of risks across business areas and reporting lines, the identification of risk interactions – including the impact of money laundering and terrorist financing risks, climate change and environmental risks, and social and governance risks on the risks directly arising from the service provision activities of the financial institution – the assessment of risks in an identical content and methodological framework within the financial institution and the group, maintaining them at the expected level and forecasting of the risks.

93. All employees within the financial institution are expected to be aware of their responsibilities related to the management of the risks of the financial institution or group.

IV.10.2 Elements of the risk management system

94. The MNB expects the financial institution to establish and operate an operational risk management function in accordance with the statutory requirements, risk policies, procedures and controls, as part of the first line of defence, as described in point 95, and a risk control function as part of the second line of defence, as an independent risk management function described in point V.4.

95. Operational risk management is responsible for implementing risk management practices complying with the statutory requirements, the financial institution's risk policy, internal procedures and established internal control processes in the day-to-day activities of the financial institution, in the individual (non-standardised) risk-taking process, in the phase lasting until the approval of the risk taking decision.

Within the framework of this, operational risk management shall perform, among others, the following tasks, based on the risk assessment of individual transactions:

- a) continuous and timely identification of risks at client or client group level, and making proposals for the management of those (mitigation or elimination),
- b) providing input for defining the risk management strategy of the financial institution or group,
- c) participating in the implementation of the risk strategy and policy,
- d) participating in the setting of risk limits at client or client group level,
- e) providing input for elaboration of risk management upon the introduction of new products and services or the modifications of existing products.

IV.10.3 General expectations concerning risk management

The financial institution or group is expected to design its limit system considering the special features of the financial institution or group. It should be aligned with the financial institution's or group's strategic objectives, risk appetite and role in the financial intermediary system, and ensure that the financial institution or group pursues its activity in compliance with the limit system and has formal procedures in place for the event of potential limit breaches.

- 96. The MNB expects that when an operational risk assumption decision is not supported by the operational risk management function under point 95 or the risk control function under point V.4, it should be rejected or the risk assumption should be escalated to a higher level, to be decided at least at committee level.
- 97. The MNB expects the financial institution to use forward looking (e.g. stress tests) and retrospective tools suitable for detecting risk concentrations as well during the identification and assessment of the risks the financial institution or group. Retrospective tools are suitable for the comparison of the risk profile and the risk appetite/risk-bearing capacity of the financial institution or group. Forward-looking tools can be used for the identification of risks that may arise in crisis situations.
- 98. When using external service providers, their analyses, methodologies, solutions, etc., the ultimate responsibility for risk assessment shall always rest with the financial institution. The MNB is of the opinion that it is not sufficiently prudent to use programmes, data and assessments (such as ratings from credit rating agencies, purchased risk models) purchased from external service providers without reviewing them and adapting them to the specific needs and characteristics of the financial institution or group.
- 99. In addition to quantitative information and data, qualitative aspects (e.g. expert valuations, presumptions and limitations of the risk assessment models) should also be taken into account when assessing risks.

100. In connection with the risk management activities, the financial institution or group is expected to have a well-defined, properly documented internal reporting system, approved by the financial institution's governing body, to provide the financial institution's management and the areas affected by risks in operational risk management and in the implementation of the risk control function with timely, accurate, transparent, understandable, relevant and useful information on the extent (size and type) of risks and on the identification, measurement or assessment of risks and their monitoring.
101. The MNB expects larger financial institutions with more complex activities – including, among others, credit institutions with a market share of over five percent based on balance sheet total – to also appoint an independent chief risk officer (hereinafter: CRO) in charge of the operative risk management function under point 95 and the risk control function under point V.4; the independence requirements under subpoints a), b), d), e) and f) of point 108 shall be enforced also in respect this executive.
102. The MNB expects the financial institution to establish a central risk management unit and – in the case of larger financial institutions with more complex activities – also a risk management committee to monitor the risk-taking strategy and risk appetite of the financial institution or group, to support the body with governance function in the implementation of the risk assumption strategy and to liaise with external experts used in the connection with the risk management activities²⁶. In addition to the foregoing, the statutory requirements may specify additional tasks for the risk committee or may further detail the general requirements (e.g. reviewing remuneration policies to ensure that the incentives in the remuneration system duly consider the risks, capital and liquidity position of the financial institution or group, the probability and scheduling of incomes, the role of the financial institution in the financial intermediary system).
103. The MNB expects financial institutions or groups to subject their risk management systems to regular internal or external audits, including an assessment of the operation in line with risk appetite and in accordance with the provisions of point 12 at a frequency and in a manner specified in the internal regulation; in this respect the MNB regards it as good practice to perform the assessment at least annually.
104. In addition to the general principles of this recommendation, risk management is also dealt with by a number of other supervisory regulatory instruments, outlining special risk management considerations in terms of managing the individual types of risks (e.g. credit risk, liquidity risk, money laundering and terrorist financing risk, climate change and environmental risks) or for individual types of financial institutions. Since the MNB deems it particularly important to enhance the risk management systems of financial institutions, it

²⁶ The establishment of a risk management committee pursuant to Article 110(1) of the Credit Institution Act is also a statutory requirement for credit institutions with a market share of at least five percent based on balance sheet total, and pursuant to Article 20/A(1) of the Investment Firms Act for investment firms with a balance sheet total exceeding HUF 200 billion.

continuously maintains the supervisory regulatory tools dealing with risk management and issues new ones when necessary. The current versions of the supervisory regulatory tools are available on the MNB website.²⁷

V. Internal control system

V.1 Expectations for the design of the internal control system

106. The financial institution is expected to establish and operate a comprehensive and efficient internal control system covering the entire organisation (including executive bodies) of the financial institution or group, all of its activities and organisational units (including those performing control functions), and to create and maintain a culture that ensures a positive attitude towards the operation of the internal control system, bearing in mind the principle of proportionality specified in point 10. The internal control system facilitates
- a) effective and efficient operation,
 - b) prudent business management,
 - c) proper identification, measuring and monitoring of risks,
 - d) reliability of financial and other information reported to internal and external users,
 - e) prudent administrative and accounting procedures,
 - f) compliance with the laws, supervisory and professional requirements and standards as well as with the internal policies, procedures, rules and decisions of the financial institution (including compliance with requirements and expectations related to the prevention of money laundering and terrorist financing).
107. The MNB expects that – bearing in mind the principle of proportionality specified in point 10 – in order to implement an efficient and comprehensive internal control system, the financial institution or group should develop and operate
- a) risk control functions,
 - b) a compliance function, and
 - c) an internal audit function.²⁸

The operation of the risk control function and the compliance function are monitored by the internal audit function.

²⁷ <http://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok>

²⁸ The provisions of the sectoral legislation also vary in respect of the internal control functions. For several types of financial institutions, certain elements also take the form of a statutory obligation.

V.2 Independence of internal control functions

108. Financial institutions are expected to guarantee the independence of certain internal control functions under point 107. An internal control function is considered independent when all of the following conditions are satisfied:
- a) the personnel of the internal control function (including its head) performs no such activities that fall within the supervisory and audit competence of the internal control function;
 - b) the area in charge of internal control is organisationally separated from the activity and organisational units it is meant to supervise and control;
 - c) the head of the internal control function may report only to a person who is not directly responsible for the management of the areas monitored and controlled by that control function;
 - d) no member of the body with governance and supervisory function may give any instruction to the area performing the internal control function which would prevent that function from carrying out any investigation deemed justified by it, or assign to the area performing the internal control function any additional tasks compared to its original work plan to the extent that this would hinder its efficient functioning;
 - e) the head of the internal control function shall be appointed directly by, or report to, the financial institution's governing body, supervisory body or audit committee through a written procedure related to the selection and appointment of the executives of the internal control functions and he shall attend at least once a year the meeting of the body that he reports to;
 - f) the dismissal of the head the internal control function is subject to the approval of the financial institution's supervisory body;²⁹
 - g) the remuneration of the internal control personnel is independent of the performance of the area audited or to be monitored and controlled, and the remuneration practices shall not compromise the objectivity of the persons performing the internal control function in any other way;³⁰
 - h) the provision of the area performing the internal control function with the resources (human and material) necessary for discharging its duties is guaranteed.
109. The MNB expects that in terms of organisation the risk control function, the compliance function and the independent internal audit area should also be independent of each other,

²⁹ This is also stipulated in legislative requirements in respect of several financial institutions and functions.

³⁰ The rules and expectations regarding remuneration are specified by the legislation applicable to the sector, MNB Regulation No 39/2014 (X. 9.), Commission Delegated Regulations 527/2014/EU and 2021/923/EU, Article 258(4) of Commission Delegated Regulation 2015/35/EU, MNB Recommendation No 3/2018 (I. 16.) – at the time of issuing this recommendation – on the remuneration policies to be applied by UCITS fund managers, MNB Recommendation No 4/2018 (I. 16.) – at the time of issuing this recommendation – remuneration policies to be applied by alternative investment fund managers, MNB Recommendation No 13/2018 (III. 6.) – at the time of issuing this recommendation – on the Remuneration policy related to the sales of retail banking products and services, and the related internal rules of procedure III.) on remuneration policies and internal rules of procedure for the sale of retail banking products and services, MNB Recommendation No 22/2019 (XII. 17.) – at the time of issuing this recommendation – on the Remuneration policy and practice to be applied in relation to the rendering of investment services, and MNB Recommendation No 8/2021 (VI. 23.) – at the time of issuing this recommendation – on the Application of remuneration policy.

as they perform different functions. The coordination of their activities should be ensured by the financial institution's governing body, supervisory body or audit committee. With regard to the implementation of organisational independence, the MNB does not regard it as good practice when the risk control function, the compliance function and the independent internal audit function are managed by the same executive; at least the internal audit function should be separated. The financial institution is expected to designate in its internal regulations the organisational units responsible for the individual control functions and the role of each organisational unit in the exercise of the individual control functions.³¹

110. Considering the principle of proportionality, at a smaller financial institution ensuring the independence of the individual internal control functions, or operating them as independent organisational units may not be justified or may run into difficulties. The combination of areas performing the individual internal control functions is also permitted by the statutory requirements subject to certain conditions. In such cases, the MNB expects the financial institution to assess the risks arising from the internal control functions' lack of independence, to take steps for managing and mitigating these risks (e.g. by duly considering this when defining decision-making procedures, joint exercise of the function by several financial institutions³²) and to pursue its activities in the knowledge of those. The financial institution is also expected to document the applied solution supported by proper justification and to present it to the MNB upon request to this effect. However – for larger financial institutions, pursuing more complex activity, including credit institutions with a market share exceeding five percent based balance sheet total – the MNB does not regard it as good practice to combine areas performing the individual internal control functions (risk control, compliance, internal audit); financial institutions are expected to establish independent organisational units for the operation of individual internal control functions, separate from each other and from other organisational units and vesting the heads of the areas in charge of the individual internal control function with sole responsibility for that function. However, the MNB does not regard it as good practice for any financial institution – with the exception of venture capital fund managers, in view of their usually small organisation and investor base – to combine the internal audit function with other internal control functions, and expects it to be operated as a separate function from the other two internal control functions at all times.
111. Statutory provisions – and consequently this recommendation as well – often assign the same task (e.g. verification of compliance with statutory requirements) to different control functions.

³¹ This is also an explicit statutory requirement for financial institutions falling within the Credit Institution Act and the Investment Firms Act.

³² Subject to statutory restrictions – for example, a bank, a specialised credit institution is obliged to operate an internal audit system.

In such cases, the financial institution is expected to stipulate in its internal regulations the division of tasks between the individual functions, the different criteria applicable to the implementation of the task by the individual functions and the expectation of effective exchange of information between the individual functions. It is also necessary to achieve the necessary harmony, efficient exchange of information and division of labour with other areas in charge of special control functions and tasks [e.g. IT security, internal data protection, fraud risk, actuarial function³³, the asset controller in the case of mortgage credit institutions, the employee responsible for the protection of clients' financial assets and funds in the case of investment firms (hereinafter: safeguarding officer³⁴)]. In view of the specific requirements to be enforced in respect of the internal audit function and in line with point 110, the MNB also does not regard it as good practice to perform other special control functions and tasks within the framework of internal audit, also considering the provisions of point 198 in respect of the safeguarding officer.

112. The governing body of the financial institution shall be responsible for establishing and operating the risk control function, the compliance function and the internal audit function in accordance with the relevant statutory requirements and for ensuring the conditions (such as the availability of appropriate authorisations and ensuring that the areas performing the internal control function can communicate directly with each other, with the relevant committee of the financial institution, the governing body and the oversight body, as necessary) and resources for their operation, as specified in point 114. Within the framework of this, – subject to considering the special rules applicable to the internal audit function – the body performing the governance function shall be responsible, in particular, for the development and communication of policies related to the individual internal control functions, the approval of internal regulations applicable to each internal control function and the implementation of the related control activities.

V.3. Common expectations regarding the functioning of internal control functions

113. Management support is a key to the operation of internal control functions. On the other hand, it is a basic requirement that the operation of internal control functions should support the governance activities of the financial institution or group.
114. The MNB expects the financial institution or group to have at all times an adequate number of human resources with the necessary skills, qualifications and authority to perform internal control functions, taking into consideration the principle of proportionality; in addition, the financial institution is expected to ensure

³³ Section 57 and 81(a) of the Insurance Act

³⁴ Section 21(2) of the Investment Services Act

the regular training of the internal control personnel and to provide them with the competence, material and IT resources, access to IT systems, databases and support, external and internal information necessary for the performance of their duties, and the possibility of relying on external experts as necessary.

115. When there is a significant increase in activities or risks, the financial institution is expected to review the operation of its internal control functions and to take steps to strengthen the individual internal control functions commensurate with the increase in activities or risks, including, among other things, increasing material and IT resources as well as human resources as necessary.
116. The MNB expects that the resources and rights under points 114, 115 and 118 are determined after consulting the head of the relevant internal control function. It is also expected that the heads of the organisational units performing the internal control function should always be informed in advance in writing, with justification, of any planned significant reduction in resources or authority affecting the internal control function.
117. Subject to compliance with the legal requirements related to outsourcing and the related supervisory regulatory instruments, in particular MNB Recommendation No 7/2020 (VI. 3.) – at the time of issuing this recommendation – on the use of external service providers [hereinafter: MNB Recommendation No 7/2020 (VI. 3.)], and the requirements specified in this recommendation with regard to outsourcing (e.g. prior management approval, ultimate responsibility for the function remains with the financial institution), the internal control functions may be outsourced in whole or in part.
118. Continuous monitoring of the changes in the regulatory environment (laws and other regulatory instruments) is essential for the operation of the internal control functions. In connection with this, the financial institution is expected to develop appropriate procedures to monitor changes in the regulatory environment. The MNB expects the financial institution to stipulate in its internal regulations the responsibilities and powers of the participants in the regulatory monitoring process (ongoing monitoring) (which is not necessarily a single function or organisational unit) and to ensure that the efficient operation of process is adequately supported by IT.
119. Those exercising internal control functions are expected to utilise the experiences gained from the in-process and management controls, and those exercising the individual functions shall cooperate with each other, learn the result of each other's work and use those in their own work. The MNB also expects the foregoing to be enforced at group level, especially in respect of the relations between bodies, organisational units and persons with the same functions at the individual group members.

120. The financial institution is expected to ensure that the head of the internal control function can attend, as he deems it necessary, as an observer the meetings of the governing body and the supervisory body and the committees referred to in point 64.
121. The MNB regards it as good practice for a financial institution or group to establish an internal reporting system covering all aspects of the operation of its internal control functions. The internal reporting system ensures the flow of information between the areas affected by or exercising the individual internal control functions. The management of the financial institution can rely on this to obtain information on the shortcomings identified by the individual internal control functions, the risks incurred and can take the necessary measures to remedy them and monitor the implementation of the measures.
122. The financial institution is expected to lay down in its internal regulations the specific rules for the termination of the mandate of the heads of the individual areas in charge of the internal control function. In connection with this, the MNB expects the financial institution to inform the MNB without delay of the termination of the mandate of the head of any internal control, specifying the reasons.

V.4 Risk control function

123. The MNB deems it important for the risk control function, ensuring the transparency of risks at the level of the financial institution or group and the monitoring of the functioning of the risk management system, designed and operated considering the criteria specified in points 124 to 127, separately from operational risk management – using an organisational, governance or other solution – to play a central role in the operation of the financial institution.³⁵ In line with the provisions of point 110, larger financial institutions³⁶, pursuing more complex activity are expected to establish an independent organisational unit or units for the operation of the function.
124. Tasks of the risk control function at individual and group level:
- a) defining the risk appetite and risk management strategy in line with the strategy of the financial institution or group (stipulating the individual types of risk rejected by the financial institution or group and the type and extent of risks it intends to take), continuous monitoring of the risks, comparing the exposure and profile with the strategy, risk appetite, policies for managing each type of risk and the limit system,

³⁵ In the case of credit institutions with a market share of at least five percent based on balance sheet total, the risk control function shall be performed by the unit responsible for the risk control function, specified in Article 111(1) of the Credit Institutions Act, covering all significant risks of the credit institution. In the case of insurance and reinsurance companies, in accordance with the Solvency II Directive, the person responsible for risk management shall perform the tasks similar to those listed in the foregoing.

³⁶ In terms of balance sheet total, the Credit Institutions Act prescribes a market share of five percent for the fulfilment of this requirement. Pursuant to Article 209(2) of the Insurance Act, in the case of insurance companies, the provisions on the operation of the risk management function shall not apply to small insurers.

- b) defining the policies for the management of the individual risk types and taking shared responsibility with the financial institution's governing body for the implementation of those policies,
- c) without assuming ultimate responsibility for the decision, participating in management decisions that have a significant impact on risk management, but not related to the implementation of policies under point b), in order to ensure that risk management aspects are integrated as much as possible in the decisions taken by the financial institution,
- d) setting risk limits other than client or client group risk limits (e.g. country limit, product limit),
- e) defining and laying down the processes, procedures, tasks, decision-making and control powers relating to the risk management system,
- f) development of the ICAAP/ILAAP/ORSA framework,
- g) development and evaluation of procedures and methodologies (including the supporting IT background) used for identifying, measuring or assessing risks and for monitoring them on an ongoing basis, in particular in terms of the appropriateness and effectiveness of the assumptions and methodologies used, and based on that identification, measurement, assessment and monitoring of risks on an ongoing and timely basis,
- h) preparing reports on risk management activities,
- i) development and implementation of procedures to be followed in the event of breaching approved risk limits,
- j) prior to the introduction of new products and services and entering new markets, as well as in the case of significant external and internal changes (including changes to the strategy, policies and limits of the financial institution or group for managing certain types of risk) and non-standard transactions, assessing and evaluating the impact on and the risks incurred by the financial institution or group and developing a plan for managing the risks incurred, based on input from operational risk management and other areas of the financial institution,
- k) identifying new or threatening processes and risks affecting the financial institution or group and its risks,
- l) identifying shortcomings and bad practices in the risk management activities of the financial institution or group and making recommendations to the management; taking actions to apply the necessary measures (e.g. developing an action plan and facilitating and monitoring the implementation of the measures specified therein),
- m) identifying and initiating the necessary actions based on the recommendations of the internal audit and the auditor regarding the management of risks, and monitoring the implemented corrective actions.

125. To this end, the MNB expects all financial institutions to designate – duly considering the potential conflicts of interest – the executive responsible for the risk control of the financial institution or group. In the case of larger financial institutions, pursuing more complex

activities – including, among others, a credit institution with a market share exceeding five percent based on balance sheet total – it is appropriate to designate a dedicated senior executive with appropriate expertise and experience to exercise or manage the risk control function³⁷, directly reporting to the CRO and who is separated from operational risk management at the level below the CRO to ensure independence. The MNB expects credit institutions, financial holding companies, mixed financial holding companies, investment firms, investment holding companies, insurance and reinsurance companies subject to consolidated supervision based on the MNB's decision to appoint a risk control manager also at group level.

126. The MNB expects that the head of a financial institution under point 125

- a) should be responsible for providing the governing body with comprehensive and understandable information on the risks of the financial institution or group,
- b) should have appropriate experience, independence and sufficiently high position – in the case of larger financial institutions with more complex activity, including, among others, credit institutions with a market share exceeding five percent based on balance sheet total, at least immediately below the level of the CRO – to be able to subject the risks of the financial institution or group with significant impact on its operation and the decisions affecting its risk framework to a preliminary critical review, which may as well include providing him with a right of veto,
- c) should be able to subject decisions taken by the management of the financial institution and its governing body, to critical review.

127. The financial institution is expected to establish and maintain appropriate internal procedures for the practice to be followed when the head of the financial institution under point 125 has expressed criticism concerning the decisions of the financial institution or group related to risks and risk management, including the cases, form and rules of granting a right of veto in respect of various decisions.

V.5 Compliance function

128. The purpose of operating the compliance function is to identify, mitigate and manage compliance risks. Compliance risk is defined as the risk of legal, supervisory or other administrative sanctions, material financial loss or loss of reputation that a financial institution may suffer as a result of its failure to comply with the laws applicable to the financial institution and other regulations not qualifying as a law – including the supervisory regulatory instruments issued by the MNB, the regulations issued by self-regulating bodies

³⁷ Pursuant to Article 111(5) of the Credit Institutions Act and Article 55(1)e) of the Insurance Act, this is also a statutory requirement for insurance and reinsurance companies.

(KELER, BSE, MABISZ), market practices, codes of conduct and ethical norms – and internal regulations (hereinafter collectively: compliance rules).

129. Compliance risks may arise – representing different weights at the different types of financial institutions – in connection with the following factors:
- a) secrecy and data protection (trade, banking, securities, fund, payments, occupational pension and insurance secret, protection of personal data) that is in line with regulation applicable to the Data Protection Officer³⁸ and with the practices applied by the financial institution,
 - b) managing conflicts of interest;
 - c) separation of financial and investment services activities;
 - d) compliance with the restrictions on the flow of information;
 - e) preventing market abuse (insider trading, unfair currency manipulation);
 - f) preventing and managing external and internal frauds;
 - g) combating money laundering and terrorist financing;
 - h) own-account transactions of the financial institution, group members and employees;
 - i) fair treatment of customers, including complaint handling;
 - j) relations with public authorities (including in particular the MNB and the Financial Arbitration Board);
 - k) conduct risk.
130. The financial institution is expected to pay special attention to developing and maintaining a compliance culture. To this end, the financial institution is expected to develop and operate a compliance function³⁹. In the course of this, not only the special features, scope and complexity of the service activities pursued by the financial institution or group should be taken into consideration, but consistency with internal governance and other internal control functions (risk control, internal audit) – subject to the provisions of point 109111 – should also be ensured.
131. In relation to the operation of the compliance function, the MNB expects that it should cover the entirety of the financial institution or group, all members, organisational units, business areas and activities of the group, including outsourced activities.
132. The MNB expects the body of the financial institution with governance function to define the compliance policy of the financial institution or group⁴⁰, which shall stipulate, among

³⁸ Act CXII of 2011 on Informational Self-determination and Freedom of Information and Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

³⁹ Pursuant to Article 153/A of the Credit Institutions Act, Article 81c) of the Insurance Act and Article 21(1) of the Investment Firms Act, this is also a statutory requirement for a specific range of financial institutions. Although the terminology used in laws applicable to the sectors varies.

⁴⁰ The development of a compliance policy is a statutory requirement only in the case of insurance and reinsurance companies. [Article 84(1)f) of the Insurance Act ⁴¹ The legislation applicable to the various sectors applies different title to the head of the compliance area.

others, the purpose, priorities and areas for the development of the compliance function, the principles governing the operation of the compliance function, the applied organisational solution, including the relationship with the governing and supervisory bodies of the financial institution, and the manner of publishing the policy.

133. The compliance policy shall define particularly the following:

- a) the requirement to ensure risk-based compliance,
- b) the management functions exercised, as part of the responsible internal governance, by the financial institution's governing body in respect of the compliance activities and types of supervisory functions enforced,
- c) the position of the manager in charge of compliance, the chief compliance officer, the compliance manager or the ⁴¹ independent organisational unit within the organisation (including, for example, the clear definition of its tasks and powers, scope of responsibility, reporting obligation),
- d) which of the compliance risks are managed primarily by the compliance function, or allocated to other audit (in-process control) or control functions (e.g. risk control function, internal audit function), and what solutions ensure communication and consistency between the different areas exercising control over compliance risks,
- e) whether the financial institution operates a compliance function as part of its operational risk management or independently of it, and what safeguards are in place to ensure the independence of the function,
- f) how the performance of the compliance function is controlled by the independent internal auditor,
- g) how (with what frequency and scope) the compliance function is exercised at the level of the financial group and for outsourced activities,
- h) conditions of relying on the services of external consultants, experts,
- i) mechanisms for reporting breaches of compliance rules⁴¹.

134. Even in the absence of a statutory obligation, the MNB expects all financial institutions⁴² to employ and designate a manager in charge of compliance, a chief compliance officer or compliance manager. However, subject to point 110, for smaller financial institutions pursuing less complex activity, the MNB deems it acceptable to manage compliance risks within the risk control function or another area that performs no internal control function (such as legal area), provided that this does not compromise the independence of that area.

⁴¹ Pursuant to Article 116 of the Credit Institutions Act and Article 24/G of the Investment Firms Act, credit institutions and investment firms shall develop effective and reliable mechanisms to encourage notification by officers and employees in the event of actual or potential breaches of the statutory requirements.

⁴² Under current legislation, this is a statutory requirement for credit institutions, investment firms, insurance and reinsurance companies (however, it should be noted that the laws applicable to the various sectors use different names).

135. The MNB expects the controlling financial institution to designate also manager in charge of group compliance, a chief compliance officer and a compliance manager responsible for ensuring the consistency of the compliance function at group level. Within the framework of this, the manager in charge of group compliance, the chief compliance officer and the compliance manager shall – subject to the relevant statutory requirements, particularly the confidentiality requirements – shall perform the following tasks:
- a) identification and analysis of group-level risks using a compliance approach,
 - b) developing uniform compliance procedures and rules, transfer of methodologies,
 - c) coordinating the activities of the compliance managers, chief compliance officers and senior compliance managers belonging to the group,
 - d) education and training at group level.
136. Where local rules applicable to subsidiaries or branches of a financial institution prevent the enforcement of more stringent group compliance principles and procedures – including in particular restrictions on the flow of information between group members – the subsidiary or branch is expected to inform the group compliance manager, the chief compliance officer and senior compliance manager accordingly.
137. The MNB recommends that the area in charge of the compliance function should carry out the following tasks⁴³:
- a) regulatory tasks:
 - aa) defining the range of the compliance rules to be applied by the financial institution or group, including the scope of information relevant for compliance,
 - ab) analysis of the potential impact of changes in the compliance rules (monitoring changes in the external and internal environment of the financial institution or group),
 - ac) participating as a reviewer in the development of policies and procedures related to the business activities of the financial institution or group, initiating necessary changes in the internal regulations and operations of the financial institution or group, and monitoring the adequacy of implementation, ad) compiling, updating as necessary and on a regular basis, the compliance policy, manual and related internal rules and regulations, including the development and documentation of methods and procedures for the identification, estimation and analysis of compliance risk;
 - b) operational tasks:
 - ba) reviewing and assessing compliance with the compliance rules (continuous monitoring) in all areas relevant to compliance risks, and reporting breaches of compliance rules to the management of the financial institution, bb) advising the management of the financial institution on compliance matters and regular reporting, bc) compliance training for the human resources of the financial institution, day-to-day availability, assistance in answering compliance-related questions from employees, bd)

⁴³ The division may be based on other criteria as well (e.g. risk management, support, reporting, monitoring).

keeping records of information relevant to compliance (e.g. employees' own-account transactions, conflict of interest notifications, insider registers) and categorising and listing data from the available database according to specific criteria, with special attention to information available in the complaint handling activities, and monitoring the records,

be) fulfilment of certain reporting obligations to the authorities (e.g. conflict of interest, money laundering, terrorist financing, insider trading, market manipulation), bf) providing a duly documented compliance opinion prior to the introduction of new products, processes or organisational changes,

bg) continuous monitoring of the complaint handling activity and utilising the information generated in the course of complaint handling,

bh) involvement in the identification and management of conflicts of interest under point IV.9 or utilising the information generated by other areas of the financial institution in the course of its activities in this respect,

bi) within the activity specified under bh) – if relevant –, involvement in the identification and management of potential conflicts of interest related to the use of external service providers, as well as in the risk assessment, due diligence and review of prospective external service providers, in accordance with the internal regulations of the financial institution, considering the provisions of MNB Recommendation No 7/2020 (VI. 3.) of 3 June 2020,

bj) in order to prevent, detect and report market abuse effectively – with due regard to the principle of proportionality outlined in point 10 – developing, operating and regularly reviewing the system under Article 16 of Regulation 596/2014/EU of the European Parliament and of the Council, which is in line with provisions of Commission Delegated regulation 2016/957/EU⁴⁴; furthermore, it takes into consideration the forms of conduct detailed in Annex I to Regulation 596/2014/EU of the European Parliament and of the Council and in Annex II to Commission Delegated Regulation 2016/522/EU⁴⁵ and the employees' own account transactions,

bk) as a good practice, participating in the review of the financial institution's communication material to customers (e.g. customer information leaflets, direct marketing, advertisements, marketing material).

138. The MNB expects the area in charge of the compliance function to carry out a compliance risk assessment as part of its duties to ensure the identification and monitoring of compliance risks. The financial institution is expected to establish a compliance risk map or compliance risk matrix for the financial institution or group based on the assessment of

⁴⁴ Commission Delegated Regulation 2016/957/EU of 9 March 2016 supplementing Regulation 596/2014/EU of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions

⁴⁵ Commission Delegated Regulation (EU) 2016/522 of 17 December 2015 supplementing Regulation 596/2014/EU of the European Parliament and of the Council as regards an exemption for certain third countries public bodies and central banks, the indicators of market manipulation, the disclosure thresholds, the competent authority for notifications of delays, the permission for trading during closed periods and types of notifiable managers' transactions

compliance risks in order to define the objectives, priorities and focus of its compliance activities, and, considering that, its work plan, tools and methods of its activities.

139. In the course of the risk assessment under point 138, the MNB regards it as good practice to use a measurement and management methodology based on severity and frequency estimates, which allows for the identification of the risk events and the estimation of their potential financial impact. The MNB also regards it as good practice for the business areas to perform self-assessment or to collect data through questionnaires prepared by the compliance function, with the proviso that when developing the risk map, the compliance function is expected to rely on objective, historical data in addition to the results obtained from the evaluation of these.
140. The MNB expects the financial institution to review compliance risk assessment regularly, at least annually, and update it as necessary to ensure that the objectives, focus and scope of the compliance function's activities remain up-to-date at all times.
141. When assessing compliance risks, the financial institution is expected to have regard to the following:
- a) laws, other external and internal regulatory instruments with compliance relevance, policies, procedures, systems and control mechanisms applied by the institution,
 - b) risks arising from legislative changes and expected new regulations with compliance relevance,
 - c) complaints relevant to compliance risks,
 - d) pending and closed litigation relevant to compliance risks,
 - e) nature, number and volume of administrative measures and sanctions,
 - f) frequency and significance of negative media coverage relevant to compliance risks affecting the reputation of the financial institution or group.
142. The tools and methods that may be used in the monitoring activities of the compliance area may include particularly:
- a) use of aggregated risk measures (such as risk indicators),
 - b) use of ad hoc reports that document material differences between the actual situation and expectations (exception reports) or situations that need to be resolved (problem logs),
 - c) monitoring procedures, reviewing documents and – where necessary, at the discretion of the compliance function, –making direct, random enquiries to the employees and external parties concerned.
143. The MNB expects the compliance function's inspections and follow-up of inspection findings not to be limited to the verification of documents, but rather those should also ascertain how relevant policies, regulations and procedures are implemented in practice.

144. Where deficiencies are identified, the compliance function is expected to make proposals to remedy those, specifying responsible persons and deadlines for completion, and to monitor the implementation of the proposed measures. The management of the financial institution is expected to be committed and to support the implementation of its proposals for the elimination of the shortcomings identified by the area in charge of compliance. Any deviation from the proposed measures shall be documented and presented in the reports under point 145.
145. The MNB expects the compliance manager, the chief compliance officer or senior compliance manager, in addition to providing ad hoc information on significant shortcomings – even in cases where there is no statutory obligation to this effect⁴⁶ – to inform, in the case of credit institutions, the governing body at least quarterly and the supervisory body at least annually, and in the case of other financial institutions the governing and supervisory body at least annually, in a summary report, on the following:
- a) a summary of the organisational structure of the compliance function, describing any material changes in the organisational framework since the previous reporting date;
 - b) results of the most recent risk assessment under point 138, any changes compared to the previous period, the risk assessment methodology and any changes made to the risk assessment methodology since the previous reporting date;
 - c) assessing the effectiveness of the control environment at the financial institution or at group level in connection with the compliance risk;
 - d) changes in the regulatory environment and the measures that have been or will be taken as a result of these changes;
 - e) a summary of the monitoring activities carried out by the compliance function, the findings of the audits, highlighting any deficiencies, risks or breaches identified during the review of the internal policies and procedures of the financial institution or group;
 - f) actions taken or being in progress in response to the deficiencies identified, the results or expected results of those and the deadlines (including the sanctions proposed by the compliance function vis-a-vis employees as part of the measures);
 - g) if, during the period covered by the report, the financial institution departed from the recommendations made by the compliance function, a description of such departure;
 - h) assessment of the work of the compliance network (if there is any at the financial institution or group);
 - i) number of complaints received during the period under review, payments made on the basis of complaints, and presentation of the problems relevant to compliance based on the analysis of complaints;
 - j) a report on the results of the training/education focusing on compliance;

⁴⁶ Pursuant to the Credit Institutions Act, the Insurance Act and Commission Delegated Regulation 2017/565/EU the preparation of an annual summary report for the governing and supervisory body is also a statutory requirement.

- k) communication with public authorities relevant to compliance;
- l) other material issues that have arisen in relation to compliance since the last report.

146. The employees of the compliance function are expected to have the appropriate qualifications, skills, knowledge and expertise to carry out their tasks. This is particularly important in the case of the chief compliance officer, given the responsibility delegated to him as a person in key position under point 85 and the strict suitability requirements applicable to him based on MNB Recommendation No 1/2022 (I. 17.).
147. The financial institution is expected to compile an employee training programme covering compliance activities, tailored to the needs of the financial institution or group, providing employees with the opportunity to attend and allocating sufficient time, budget and resources. In addition to the training of new entrants, the financial institution is also expected to organise regular refresher trainings and, where necessary, additional in-service trainings for employees, at least annually, to provide the necessary knowledge for the detection of compliance risks. Special training activities for the employees in the compliance area are justified in order to keep their knowledge up-to-date and to familiarise them with possible new compliance methodologies and requirements.
148. The MNB expects financial institutions to organise training related to compliance activities, under point 147, also for external service providers performing intermediary activities for the financial institution and performing activities qualifying as outsourcing of critical or important functions or highly important functions or activities, as specified by the relevant statutory requirements and in MNB Recommendation No 7/2020 (VI. 3.).
149. The MNB regards it as good practice to establish a network supporting the compliance function within a financial institution or group. The members of this network are employees from areas other than compliance, supporting the management of compliance risks, monitoring the expectations of the compliance area, participating in risk assessment, supporting fraud prevention, detection, management and compliance investigations in accordance with point VII.5, in a defined percentage of their working hours. The operation of the network shall not prejudice the primary responsibility of the compliance area for these tasks.
150. Where the financial institution operates such network, it is expected to provide the respective employees with appropriate education and training necessary for the performance of their duties and to include their duties in their job descriptions. In addition, the head of the compliance function is expected to participate in the performance assessment of the network members' tasks carried out to support the network.
151. Where it is relevant to the position of the investment service provider (e.g. considering its role as a product manufacturer or distributor), the section of the investment service

provider's annual report on product governance rules is expected to cover the following items in respect of the compliance function:

- a) the role of the compliance function in developing, monitoring and reviewing the investment service provider's product governance policies and procedures,
- b) all topics related to the monitoring of the investment service provider's product governance by the compliance function area as prescribed in Article 22(2) of Commission Delegated Regulation 2017/565/EU (for example, the findings of the compliance function in relation to the investment service provider's product governance policies and procedures, breaches and deficiencies detected and corrective actions taken or to be taken in relation to the latter),
- c) information regularly provided on the financial instruments produced and distributed by the investment service provider⁴⁷, including information on the distribution strategy, for the purpose of assessing whether the product governance function of the investment service provider is functioning as intended, including at least the following:
 - ca) the number and nature of the products produced distributed, including their relevant target markets and other information from the product approval process necessary to assess the product's compliance risk, i.e. information relating to the investment service provider's product governance policy (e.g. product complexity, the conflict of interest associated with the product, especially relevant data from scenario analysis, the cost-to-income ratio), with special emphasis on new types of products produced or marketed during the reporting period, as well as information the characteristics of which have changed significantly during that period,
 - cb) in the case of the producers of the product, as part of the information on the relevant distribution strategy: the distributors involved, with special emphasis on new distributors,
 - cc) whether and to what extent the products are marketed outside their (positive) target market.

152. In order to comply with the requirement specified in subpoint c) of point 151, the compliance area may subject the work, reports and methods of the investment service provider's product governance function area or employees to inspection. In line with the principle of proportionality, for example, when reporting on the product governance rules of the investment service provider, information on simpler, more common products may be less detailed, since the complex and risky products with other characteristics (such as liquidity shortage and innovation) may need to be described in more detail.

⁴⁷ Section 4(2) and 8(8) of the Decree No 16/2017 (VI. 30.) of the Minister for National Economy on the product approval process to be used by the investment firms.

V.6 Internal audit function

153. The purpose of the internal audit function is to provide independent, objective assurance through its audits that effective set-up and operation of the internal control system (risk management, control and governance processes) ensures the realisation of the institution's objectives.

An additional purpose of operating the internal audit function is to add value and improve the quality of the organisation's operations through these audits and advisory activities.

154. The MNB expects the internal audit to cover the financial institution or group as a whole, all members of the group, its organisational units – including areas with internal control functions and areas with special control functions, such as the safeguarding officer – its business areas and activities – including outsourced activities – and their separate and matching operations.

155. The assurance activities of internal audit may include especially the following:

- a) regular analysis, inspection and assessment of the structure and operation of the internal control systems, their compliance with the laws and other non-legislative requirements – including the supervisory regulatory instruments issued by the MNB – and internal regulations as well as the of the economy, cost-efficiency and effectiveness of their operation;
- b) analysing and verifying the management of available resources, the safeguarding and augmentation of assets, the adequacy of the accounts and the authenticity of the financial statements;
- c) formulating findings, conclusions and recommendations in relation to the audited processes, in order to terminate, eliminate or reduce risks and deficiencies, prevent or detect irregularities, enhance the effectiveness of the financial institution or group and improve and develop internal control systems;
- d) designation of responsible persons and a deadline for implementing the proposals and measures or making proposals for them;
- e) keeping records and follow-up of actions taken based on internal audit reports.

156. The assurance activity shall be carried out by the financial institution, by applying, individually or in combination, especially the following audit types:

- a) the purpose of the compliance audit is to assess whether the operation and activities of the respective organisational unit or business area is adequately regulated, and whether the provisions of the prevailing laws, internal regulations and management decrees as well as the requirements of the supervisory regulatory instruments are enforced;
- b) the purpose of the financial audit is to verify the financial settlements of a financial institution, group, organisational unit, business area, programme or function as well as the underlying accounting records and the related supervisory data supply;

- c) the system audit shall include a comprehensive inspection of the design and operation of each system;
- d) the purpose of performance audit is to determine whether the operations and the use of resources in a well-defined area of the activities and programmes carried out by a specific organisational unit or business area are implemented economically, efficiently, in appropriate quality and effectively;
- e) the IT audit focuses on the adequacy, reliability and security of the information systems in the financial institution or group as well as on the completeness, appropriateness, regularity and protection of the data stored in the systems⁴⁸.

157. The tasks of internal audit carried out in an advisory capacity – implemented in a way that does not breach its independence and prevents the risk of self-audit, and without participating in the development, selection, definition and implementation of policies, mechanisms and procedures and risk limits – may include especially:

- a) supporting managers by analysing, evaluating, testing and assessing the risks of individual optional solutions;
- b) advising on more rational and efficient management of financial, material, IT and human resources;
- c) providing expert support to management in the development and continuous improvement of risk and irregularity management systems and performance management systems;
- d) advising on the streamlining of organisational structures, change management;
- e) consulting and advising the management on the elaboration of the organisational strategy;
- f) formulating proposals with regard to the content and structure of internal regulations to improve quality assurance, increase the profitability of the financial institution or group, and to improve and enhance internal control systems.

158. The MNB expects the financial institution to lay down the purpose of operating the internal audit function, its powers, responsibilities, tasks, elements, organisation and professional requirements towards the management of internal audit in an internal audit policy (charter, internal audit charter) approved by the supervisory body of the financial institution. The MNB also expects the financial institution to ensure that the rules of procedure applicable to conducting audits, the availability of the necessary IT and technical conditions for this purpose are laid down in a regulation approved by the financial institution's governing body and reviewed at least annually⁴⁹.

⁴⁸ Related recommendation: Recommendation No 8/2020 (VI. 22.) – at the time of issuance of this Recommendation – of the Magyar Nemzeti Bank on the protection of information systems

[hereinafter MNB Recommendation No 8/2020 (VI. 22.)]

⁴⁹ In the case of credit institutions, insurance and reinsurance companies, the approval of the internal audit regulation by the governing body (board of directors) and its annual review is also a statutory requirement.

159. In addition to complying with the relevant legislation, the MNB expects the operation of internal audit to comply with an international internal audit standard, in accordance with the principle of proportionality specified in point 10. In this respect, the MNB recommends to comply with the practical standards and guidelines issued by the IIA (Institute of Internal Auditors) and published by the Hungarian Organisation of Internal Auditors (BEMSZ), and to comply with the provisions of the IIA Code of Ethics.
160. In line with established international standards, the MNB also regards it as best practice to develop and operate a risk-based internal audit built on the data in the databases of the financial institution or group, supported by a risk analysis including an annual audit plan based on the audit objectives and approved by the appropriate body, and a detailed audit programme.
161. It is a basic expectation of the MNB that all financial institutions should employ an internal auditor regardless of any statutory obligation. This also applies to insurance associations, fund managers and voluntary mutual funds (part-time employment or employment under an agency contract is also acceptable in the case of small financial institutions). The MNB is of the opinion that the employment of an internal auditor serves the interest of both the MNB and the financial institution since the internal auditor acts as a critical line of defence, inspecting the activities of the financial institution and drawing attention to any incorrect practices that may infringe the law.
162. Where the size of the financial institution or the statutory requirements do not necessitate the employment of several internal auditors and the organisation employs only one internal auditor, the requirements applicable to the internal audit organisational unit or its head shall apply to the internal auditor. If several financial institutions employ the same person as internal auditor – as permitted by the law – they shall agree in writing that they will not object to the mutual employment of the internal auditor. It should be specified in the agreement that the job descriptions of internal auditors must not contain elements that lead to a conflict of interest or prevent the segregation of separate functions.
163. The MNB expects the internal auditor's activities to be independent of the areas and activities he is required to audit. To ensure independence, the internal auditor shall not be entrusted with any task other than auditing which could lead to a conflict of interest. Additional audit tasks for the internal audit organisational unit compared to the annual plan may only be prescribed by the supervisory board, its chairman, or – in connection with its duties – by the audit committee, its chairman, the head of the internal organisational unit alone or by the chief executive (executive director or the chairman of the board of directors in the case of funds) with the consent of the chairman of the board of directors or the audit committee. The head of the internal audit unit shall report to a management level that enables the internal auditor to perform his duties. The internal audit shall act independently,

within the framework defined by the governing body, when planning its activities, implementing the audit programme, selecting the methods and procedures, and it shall draw up, free from influence, an audit report containing the findings, conclusions and recommendations, and it shall be responsible for the content of such report. In order to ensure independence, the MNB recommends that the consultation on the findings of the audit report with the audited area should be properly documented at all times, and that changes and amendments made to the audit report should be recorded applying track changes.

164. The financial institution's governing body shall be responsible for ensuring the independence of internal audit, both in terms of its powers and organisation, and for ensuring that internal audit has the resources at its disposal. The governing body of the financial institution is expected to determine and make available the internal audit resources in accordance with the special features, scope, complexity and risks of the service activities of the financial institution or group and taking into consideration the international standards specified in point 159.
165. It shall be also ensured that the internal audit function has access to all information and documents necessary for the performance of their duties, it is informed of all decisions and resolutions of the governing body or management relating to the conduct of business, it can ask any person for information, has access to all premises, and may ask for statements, certificates and take minutes.
166. The MNB expects the management of the financial institution to support the internal audit activity by all available means. As part of this, the financial institution is expected to establish and maintain a culture, processes and procedures which ensure that audit findings are treated with appropriate priority and that the financial institution takes the actions required to eliminate the identified shortcomings within the prescribed timeframe. The MNB expects the financial institution to develop a formal system to follow up the internal audit recommendations and to eliminate the identified shortcomings.
167. The persons involved in internal audit activities shall collectively possess or acquire the expertise, experience and other knowledge necessary to perform their duties, thereby ensuring that the internal audit organisation as a whole is capable of auditing all activities and organisational units of the financial institution. The internal auditor shall carry out his duties with competence, due diligence, due care and professionalism.
168. In view of the rapid development of financial markets, it is a key expectation toward the internal auditors of financial institutions that they should continuously enhance their expertise, practices and other knowledge. To this end, the MNB encourages the internal audit staff to obtain Qualified Internal Auditor or Certified Internal Auditor (CIA) qualification.

169. The MNB also expects the internal audit of the financial institution to monitor regularly the soundness and reliability of the supervisory data supply – with special regard to the level of internal regulation, accounting soundness, completeness, integrity, closed nature, IT soundness, and the criteria of the operation of processes and control systems – and, in order to remedy systemic deficiencies and infringements identified by the MNB, to verify the timely completion of the tasks prescribed in MNB’s decisions or management letters concluding the audit, and to monitor whether the financial institution has taken all measures to correct the errors and mitigate the identified risks.

VI. Relationship between the financial institution and the elected auditor

170. In a narrow sense, the services provided by the auditor do not constitute an element of the internal lines of defence of the financial institution, but they represent a kind of transition between the elements constituting the internal and external lines of defence and are linked to the governance and control functions at several points. For this reason, the MNB considers it appropriate to also formulate its key expectations regarding the relationship between a financial institution and its elected auditor in this recommendation.
171. The MNB expects the financial institution to act with due diligence – through or involving its authorised bodies – upon electing the auditor, also taking into consideration the provisions of Regulation 537/2014/EU of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC, and to evaluate his activity with the frequency and in the manner stipulated in its internal regulation. To this end, the MNB recommends that the financial institution should apply an open and transparent tender procedure for the selection of the auditor.
172. The financial institution is expected, upon the election and evaluation of the auditor, through or with the involvement of its authorised bodies, to
- a) verify whether on the basis of the register of auditors authorised to carry out the audit of financial entities the auditor can be entrusted with the performance of audit and other services,
 - b) assess, on the basis of the available information, the restrictive and conflict of interest conditions specified in the sectoral and related legislation or in any other manner (e.g. ethical standards),
 - c) summarise its past experience with the auditor, available market information, reputation and assess whether the auditor’s remuneration is commensurate with the volume and professional quality of the work to be performed or performed in the past.

173. Where an audit firm has been elected as auditor, the MNB recommends that, with regard to the natural person auditor nominated by the audit firm, the financial institution should ensure that the statutory change of the natural person auditor at specific intervals results in a change in the person who performs the audit function, not only in formally but effectively as well. When deciding on the replacement of auditors, the MNB expects the financial institution to obtain reasonable assurance that the natural person appointed as the new auditor within the contracted audit firm is able – both in professional terms and in terms of close family relationships – to perform his work in a professional and independent manner, free from the influence of the previous auditor. If any doubts arise about independence, the MNB expects the natural person auditor to be replaced.
174. In the case of a financial group, the MNB expects that the conflicts of interest related to the audit activity are also managed at group level.
175. The MNB recommends that the financial institution should disclose in the annual report the type of orders given to specific auditors, applying at least the breakdown by statutory audit activity and other professional services outside the statutory audit activity, as specified in Article 3 of the Audit Act.
176. In the case of a financial group, disclosure should also include a description of the audit relationships of the group members.
177. The financial institution, through or with the involvement of its authorised bodies, is expected to make efforts to comply with the following corporate governance principles in its relationship with the auditor:
- a) recognise and communicate the importance of audit activity within the organisation;
 - b) assess compliance with the rules specified in the Audit Act and in the sectoral legislation to ensure the independence of the audit function, including in particular the rules on conflicts of interest and the rotation of auditors;
 - c) substantive review and utilisation of the audit findings, including those contained in the management letter;
 - d) take timely and effective action to remedy shortcomings based on the audit findings;
 - e) foster the review of the records, data supply, disclosures⁵⁰ and the internal control systems by the auditor;
 - f) make effort to obtain widest possible certification of the disclosed information by the auditor,
 - g) actively support the auditor in the compilation of the special auditor's report.
178. It is expected that, in order to ensure the most effective operation of external and internal controls (e.g. ownership controls), the internal audit and – if the financial institution has one

⁵⁰ Pursuant to Article 263(3) of the Credit Institutions Act, this is also a statutory obligation for credit institutions.

– the audit committee of the financial institution should maintain a good professional relationship with the auditor, in accordance with the principles set out in the Hungarian National Auditing Standards.

179. The financial institution is expected to participate and cooperate in the personal meeting between the MNB and the auditor – as requested by the MNB – in accordance with the relevant guidelines of the European supervisory authorities⁵¹.

VII. Specific issues relating to the establishment and operation of internal defence lines

VII.1 Outsourcing⁵², involving external experts

180. The MNB expects the financial institution or group to have an outsourcing policy approved by the governing body.
181. In the outsourcing policy, which covers both external and internal outsourcing through group members, the financial institution or group should define the services, activities and functions it intends to outsource, in compliance with the statutory requirements applicable to the sector⁵³, and assess the impact and risks of outsourcing on the operations of the financial institution or group, define the principles and criteria for the selection of the undertakings to conclude outsourcing contracts with.

In respect of the latter, the MNB regards it as good practice for financial institutions to verify in all cases whether the company performing the outsourced activity has appropriate ethical standards and business management practices in place before concluding the outsourcing agreement.

182. The financial institution shall determine its outsourcing policy with a view to ensuring that the outsourcing of a service, activity or function does not hinder the exercise of the internal control functions and external audit of the financial institution or group, including cooperation with the MNB and the application of supervisory measures.
183. The MNB also expects the financial institution to specify in the outsourcing policy the internal governance and control requirements arising in connection with the outsourcing activity.

⁵¹ Guidelines on communication between the competent authorities supervising credit institutions and the statutory auditor(s) and audit firm(s) carrying out statutory audits of credit institutions EBA/GL/2016/05); Guidelines on facilitating an effective dialogue between competent authorities supervising insurance undertakings and statutory auditor(s) and the audit firm(s) carrying out the statutory audit of those undertakings (EIOPA-16/858)

⁵² MNB Recommendation No 7/2020 (VI .3.) contains additional requirements on the topic of outsourcing.

⁵³ Pursuant to the Credit Institutions Act only activities involving data management or data processing may be outsourced.

184. The MNB expects the financial institution or group to review and amend its outsourcing policy, as necessary, regularly at least every five years – unless a more frequent review is justified based on the relevant statutory requirements and the requirements of MNB Recommendation No 7/2020 (VI. 3.) – or whenever a significant event relevant to the outsourcing practice occurs that affects the financial institution or group.
185. Upon outsourcing any activity, within the framework of the outsourcing policy, the financial institution is expected to take into consideration the governance and control aspects that constitute the internal lines of defence, conclude its specific outsourcing contracts with due regard to those and manage the outsourced services, activities and functions accordingly. When outsourcing any service, activity or function permitted by the law, it shall be taken into consideration that the responsibility for that service, activity or function remains with the management of the financial institution and that the legal requirements and other expectations (including this recommendation) applicable to that service, activity or function remain in force.
186. The MNB also expects financial institutions to enforce internal governance and control aspects when using external experts and consultants, which does not qualify as outsourcing, and to bear in mind the principle that the legal requirements and other expectations (e.g. usual practices, ethical rules) applicable to the respective service or activity still need to be enforced.

VII.2 New products and services

187. The MNB expects the financial institution or group to have a new product policy approved and regularly reviewed by the governing body; in this respect the MNB regards it as good practice to review the policy at least annually.
188. In the new product policy, the financial institution specifies the definition of a new product, service and market used consistently by the financial institution or group as a whole and the criteria for deciding whether to introduce a new product, service, enter a new market, or to make significant changes to existing products, services and markets (for example, establishing a new subsidiary or special purpose vehicle). The new product policy ensures that approved products and changes are in line with the relevant statutory requirements and related supervisory regulatory tools⁵⁴, the risk strategy and risk appetite of the financial institution, the related limits, and that the necessary review of related processes (e.g. risk management) and systems (e.g. IT background) is carried out at all times.

⁵⁴ The requirements for capital market service providers are specified in the Investment Firms Act. and in MNE Decree No 16/2017 (VI. 30.) on the product approval process to be applied by investment firms, while further requirements are prescribed by the MNB Recommendation on the product approval requirements for capital market services, currently under development. The statutory provisions applicable to insurers are specified in Article 131/A of the Insurance Act and Commission Delegated Regulation 2017/2358/EU of 21 September 2017 supplementing Directive 2016/97/EU of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors.

189. The MNB expects the financial institution to designate in its new product policy the decision-making processes and procedures for the introduction of new products, including the identification of the areas involved in the decision-making process, and the related internal control requirements such as risk control, compliance and the role of internal audit in approving or monitoring the application of the new product policy.
190. It is recommended that, before launching a new product or service or entering a new market, the financial institution should assess especially the following aspects: a) legal compliance, b) appropriateness of pricing models, c) impact on the risk profile, capital adequacy, liquidity and compliance with other prudential requirements and profitability of the financial institution or group, d) risks incurred – including operational risks – and the tools and capacities available to understand, monitor and mitigate those risks where necessary, e) factors that may hinder the exercise of internal control functions, f) socio-economic conditions, potential changes in those, the cyclical position of the financial system and the real economy, and g) risk of money laundering and terrorist financing and measures to mitigate these risks.

VII.3 Disaster recovery and business continuity plans

191. The MNB expects the financial institution to develop, in addition to the contingency and service continuity, business continuity and IT disaster recovery plans prescribed by the law, also a recovery plan covering the financial institution and the group as a whole with a view to preparing for emergency situations – occurrence of emergency, steadily restricted access to critical resource and disruptions in the financial institution's services as a result of those – and mitigating the operational, financial, legal, reputational and other material consequences of those.⁵⁵
192. In the contingency and service continuity plans, the financial institution reviews the potential actions it may need to take to maintain the continuity of key business activities (e.g. accounting processes) and functions (e.g. operation of IT, communication systems) in the event of an emergency⁵⁶.
193. A recovery plan is a plan of measures that ensure the stabilisation of the financial situation of a financial institution or group in the event of a situation that poses a serious threat to liquidity or solvency, without recourse to extraordinary financial assistance from the

⁵⁵ This is also a statutory obligation of credit institutions, pursuant to Article 114(1) of the Credit Institutions Act and of investment firms pursuant to Article 102(1) of the Investment Firms Act. The recovery plan to be prepared in advance is not the same as the plan regulated by Articles 309, 312 and 316 to 318 of the Insurance Act.

⁵⁶ Related recommendation: MNB recommendation No 8/2020 (VI. 22.)

government or to an extraordinary liquidity facility from the MNB acting in its capacity as central bank. Within the framework of preparing a recovery plan, the tools available to the financial institution or group to deal with stress situations at systemic, financial institution or group level to return to normal business operations and the potential ways of applying those are assessed. The MNB treats the preparation of recovery plans by institutions falling within the CRR is treated based on separate guidelines⁵⁷.

194. The MNB is of the opinion that by integrating the plans to be prepared in advance (such as the liquidity contingency plan) into a common preventive recovery plan it is possible for the financial institution and the group to prepare consciously for a wide range of crisis situations.

In connection with this the MNB regards it as good practice to develop and operate a separate service continuity function, for example as part of the risk control function.

195. Adequate level of documentation and approval, physically separated storage – on paper or on separate data carrier – also accessible when the IT system is down –, and providing access in emergency situation in due course, along with regular, at least annual, testing, including the documentation and analysis of the identified shortcomings, and review together with the implementation of related communication and trainings is a practice to be followed in the case of contingency and service continuity plans as well as in the case of recovery plans.

VII.4. Safeguarding officer

196. The investment service provider shall appoint a safeguarding officer with sufficient powers and expertise, responsible for the protection of customers' financial assets and funds. It is the general expectation of the MNB that the monitoring of the internal workflows and operation of IT record-keeping systems connected to the fulfilment of statutory requirements related to the management of customers' financial assets and funds along with the monitoring of cooperation with third parties and the relevant decisions and relevant practice of communication with customers should be concentrated within the duties of the safeguarding officer, in line with the provisions of point 111 and point 137b)bj). The MNB expects – in line with the provisions of point 111 – that the safeguarding officer function should be performed either independently or as part of an internal control function. With regard to the latter, the MNB regards it as good practice – in line with the logic of the Investment Firms Act in force since 3 January 2018, which regulates the position immediately after the compliance function – if this function forms part of second-level internal line of defence (compliance function, risk control function), The MNB expects the safeguarding officer to report directly to the investment service provider's supervisory body on a quarterly

⁵⁷ MNB Recommendation No 8/2022 (V. 13.) – at the time of issuing this recommendation – on the recovery plan to be prepared by credit institutions and investment firms

basis, and his annual work plan and specific tasks should be defined and approved by the supervisory body. The MNB expects that the procedures for the performance of the duties of the safeguarding officer function as well as the responsibilities and powers associated with the function should be laid down in an internal policy also approved by the supervisory body.

197. Depending on the decision of the investment service provider, the duties assigned to the safeguarding officer position may be performed by the appointed person as a sole function or in combination with other functions. The MNB expects the service provider managing the assets of customers to decide, in proportion to the size of its activity – with special regard to the size of the customer assets managed and the customer base as well as the diversification of the latter, the number of the sub-custodian and settlement partners used, the complexity of the sub-custodian chain, the regular reconciliation and segregation duties along with the complexity of the infrastructure and organisation serving it – and giving due consideration to compliance with the statutory and supervisory requirements, whether the tasks belonging to the safeguarding officer position should be performed as a separate duty or supplementing the tasks of an employee performing some other internal control function. If the investment service provider opts for the latter solution, the MNB expects that the job description of the person appointed as safeguarding officer should specify this position and the related duties, specifically by name and separately from other duties.
198. The MNB expects the investment service provider to determine the number of positions allocated to fulfilling the duties connected to the safeguarding officer function with due consideration to the proportionality criterion. The investment service provider should not seek to comply only with the minimum statutory requirement when establishing the position. The MNB expects that organisational decisions concerning the safeguarding officer's function and duties should be submitted to the supervisory body. The MNB expects the investment service provider to appoint a person to perform the duties associated with the position of safeguarding officer who has comprehensive expertise in the legal requirements concerning the management of customer assets and financial instruments, the processes and functions within the organisation relating to the management of customer assets (e.g. regular reconciliation, segregation of own and customer assets, operation of record-keeping systems, business relationship with sub-custodian and settlement partners). Where the effective and sufficiently competent performance of the duties associated with the position of safeguarding officer justifies it – e.g. as a result of previous quarterly audit practices relating to the safeguarding of customer assets – the investment service provider may decide to entrust the position to a member of staff in the internal audit organisational unit. In this case, however, the MNB expects that the tasks related to the safeguarding officer position are carried in an independent position separated from other internal audit tasks. However, the MNB expects investment service providers to strive in the medium term to ensure that the safeguarding officer function is independent of the internal audit function, also considering the requirement of sufficient expertise and powers.

199. The MNB is of the opinion that the safeguarding officer has sufficient powers to perform the tasks related to the safeguarding of customer assets if, in addition to his subsequent control tasks, he has the right to provide an in-process opinion on business and organisational decisions related to the management of customer assets (e.g. introduction of a new record-keeping system, integration of record-keeping systems, selection of a new sub-custodian, conclusion of collateral agreements, decisions affecting the relevant organisational units in respect of statutory requirements for the management of client assets). The supervisory authority also expects the safeguarding officer to have access rights to IT systems related to the management of customers assets to ensure the independent performance of his inspection and review tasks and information on the business and organisational decisions related to the management of customer assets.
200. The MNB expects that the duties of the safeguarding officer appointed by the investment service provider cover at least the following tasks:
- a) continuous, traceable and documented monitoring of the statutory provisions – particularly those specified in Articles 57 to 60 of the Investment Firms Act – related to the management of customers’ financial assets and funds along the supervisory requirements specified in the relevant management circulars⁵⁸, including the conduct of an itemised detailed cash and securities collateralisation audit and the preparation and submission of a quarterly report on the audit to the MNB;
 - b) participating in the development of selection and qualification practices for third parties entrusted with the management and registration of customer assets, providing opinions on these practices, participating in the implementation of regular counterparty reviews, providing opinions on contracts with third parties, and reviewing contractual documentation;
 - c) monitoring and regularly reviewing the in-process mechanisms – particularly those preventing unauthorised access – for the protection of clients’ financial assets and funds, and developing and commenting on practices, policies and agreements relating to the use of customer assets, including, where relevant, participation in the development of the conditions for the application of collateral agreements with transfer of ownership;
 - d) contributing to the development of the information provided to customers on the protection of customer assets, expressing opinion on it;
 - e) conducting documented internal training for employees on the protection of customers’ financial assets and funds;
 - f) developing and operating an internal reporting process for any events that lead to breaches of the statutory requirements relating to the management of customers’ financial assets and funds, or threaten the protection of customers’ assets or their right

⁵⁸ <https://www.mnb.hu/letoltes/tmpb0a8-tmp-14558992.pdf>, valamint a 63538-2/2016 iktatószámú vezetői körlevél

to dispose over them, recording, promptly investigating and reporting notifications to the governing body and, simultaneously with that, to the supervisory body and, on a quarterly basis, to the MNB, and proposing measures and monitoring their prompt implementation;

-
- g) if the investment service provider is unable to rectify immediately the situation that threatens the protection of customer's assets in relation to the case detected in accordance with subpoint f), providing the MNB with direct, detailed and written information on the identified risk.

201. The internal audit of the investment service provider is expected to verify, at a frequency proportionate to the activities of the financial institution or group, on a quarterly, semi-annual or annual basis, that the safeguarding officer's activity complies with the requirements of this recommendation and to report annually to the bodies he is subordinated and reporting to. Upon compiling the audit plan under point 160, the investment service provider is also expected to take into consideration the special supervisory requirement to be enforced in respect of this function.

VII.5 Fraud prevention and management

202. The MNB expects the financial institution to act in accordance with the related supervisory regulatory instruments⁵⁹ with regard to the prevention of fraud, the management of realised frauds and attempted frauds, which failed due to the proper functioning of controls or due to other reasons, or which have been prevented, in accordance with the principle of proportionality specified in point 10, and taking into consideration the principles outlined in this recommendation.

203. The MNB expects financial institutions to develop a culture of fraud prevention and management that strives for zero tolerance of fraud and primarily focuses on fraud prevention. The primary means of creating and maintaining a strong fraud prevention and fraud management culture include internal policies, regulations, guidelines, internal and external communication and the training of employees.

204. The MNB expects that the commitment of a financial institution's executive to preventing and mitigating fraud should be transparently reflected in their governance, control and monitoring activities.

⁵⁹ At the time of issuing this recommendation, in particular: MNB Recommendation No 8/2020 (VI. 22.) and MNB Recommendation No 11/2020 (X. 20.) on the conditions of managing physical security and human risks threatening the operation of financial institutions.

VII.5.1 Training

205. The financial institution is expected to compile an employee training programme covering fraud prevention and fraud management, tailored to the needs of the financial institution, the group, the individual organisational units and jobs, providing employees with the opportunity to attend and allocating sufficient time, budget and resources. In addition to the training of new entrants, the financial institution is also expected to organise regular refresher trainings and, where necessary, additional in-service training of employees, at least annually. The MNB expects the training to cover fraud incidents that have been detected and are considered typical, fraudulent practices, fraud prevention and management methods, procedures and practices used by the financial institution. The training should transfer specific, more detailed and broader knowledge required for the employees involved to the largest degree in fraud prevention and management.

VII.5.2 Fraud prevention and fraud management strategy and policy

206. The MNB expects the financial institution to have a fraud prevention and fraud management strategy and policy, defined in accordance with the proportionality principle specified in point 10 and approved by the governing body.
207. The controlling financial institution is expected to define its fraud prevention and fraud management strategy and policy also at group level.
208. The fraud prevention and management strategy and policy is expected to cover the entire organisation of the financial institution or group – including its management bodies and the organisational units performing internal control functions – all activities and services, all persons involved in the processes and activities of the financial institution and all persons with an employment or other legal relationship with the financial institution, including external service providers.
209. The financial institution or group is expected to develop its fraud prevention and fraud management strategy and policies in line with its operational risk and compliance strategy. The MNB regards it as good practice for the strategy to include an assessment of current practices in fraud prevention and fraud management, the survey of anticipated fraud trends, the financial institution's involvement, responses to trends, and the definition of related objectives and tasks.

VII.5.3 Principles of internal regulation related to fraud prevention and fraud management

210. The MNB expects financial institution to lay down in its internal regulation related to the prevention and management of frauds at least the following:

- a) the definition of fraud risk, types of fraud risk, distinguishing in particular between external and internal fraud,
- b) the role of the executive bodies in preventing and managing fraud affecting the financial institution,
- c) governance and internal control requirements for the prevention and management of frauds,
- d) the role of the individual organisational units and internal control functions in the prevention and management of fraud (tasks, procedures, responsibilities and powers), assigned to the main successive stages of the process model i.e. prevention, surveillance or detection, investigation,
- e) the methods and procedures used for fraud prevention,
- f) tools for the detection and disclosure of potential or actual fraud,
- g) procedures, responsibilities and powers for reporting potential or actual fraud,
- h) principles, methods and procedures, responsibilities and powers for investigating suspected fraud,
- i) where relevant, the criteria (e.g. type of event, magnitude) and scope of suspected fraud events, where it is justified to decide on the application of measures at committee level,
- j) in the case specified in subpoint i), the composition and powers of the committee,
- k) specific provisions for the prevention and management of internal fraud,
- l) measures relating to the risk of fraud, rules related to recording and monitoring the applied measures,
- m) regular and extraordinary internal and external reporting requirements related to fraud risk (e.g. to whom, how often and what kind of reports are prepared, who is responsible for preparing the reports, format and content requirements, reporting lines),
- n) the way and form of communication between organisational units and internal control functions on fraud prevention and fraud management,
- o) internal audit tasks, procedures and systems related to the prevention and management of fraud (in-process, management control and internal audit tasks),
- p) record-keeping and documentation requirements related to fraud risk.

211. A financial institution is expected to define the notion of fraud risk in accordance with the statutory provisions governing the management of operational risk and the notion of fraud used in the management of its operational risk, but in a manner that is clearly distinguishable from other forms of corrupt practices defined for other purposes and adapted to its specific characteristics. The MNB also expects that the definition of fraud risk by the financial institution should extend beyond the forms of abuse defined in Hungarian criminal law to cover all intentional and unlawful corrupt practices, acts, deceptive conduct and omissions committed directly or indirectly for the purposes of unlawful or unjust enrichment or advantage through the services of the financial institution, utilising or misusing the financial

institution's procedure, instruments or system, to the detriment of the financial institution, its customer or other third parties. Damage may include an actual financial loss, a quantifiable unrealised financial benefit or non-financial (e.g. reputational) damage.

212. The financial institution or group is expected to review its fraud prevention and fraud management strategy and policies and related internal regulations on a regular basis – where the MNB regards it as good practice to perform the assessment at least annually – and whenever a suspected fraud event is considered significant, according to criteria defined by the financial institution.

VII.5.4 Organisational framework

213. The governing body of the financial institution (usually the board of directors) is expected to
- a) develop a fraud prevention and fraud management culture across the financial institution or group,
 - b) approve the fraud prevention and fraud management strategy and policy and the related internal regulations,
 - c) be responsible for ensuring that the management of the financial institution takes the necessary steps to implement a strategy and policy for the prevention and management of fraud and to monitor and control of potential or actual fraud,
 - d) exercise effective supervision of the fraud prevention and fraud management activities of the financial institution or group,
 - e) initiate, where necessary, changes to procedures and methods for fraud prevention and fraud management and to internal regulations.
214. The management is responsible for the practical implementation of the fraud prevention and fraud management strategy and policy, and for ensuring the human, material and operational conditions for the implementation. To this end, the management should establish and operate an appropriate control system, pursue management and control activities, and submit regular and comprehensive reports to the board of directors and the supervisory board on the implementation of the fraud prevention and management strategy and policy.
215. The financial institution or group is expected to develop its organisation and operational rules for fraud prevention and fraud management, and the related powers and responsibilities duly considering the principle of proportionality specified in point 10.
216. In accordance with the MNB's expectation, and bearing in mind the principle of proportionality specified in point 10, the financial institution may also establish an independent competence centre or organisational unit to coordinate the tasks related to the

prevention and management of fraud, or designate an area with an internal control function (compliance function or risk control).

217. When relying on the services of an external service provider – taking into consideration MNB Recommendation No 7/2020 (VI. 3.), where relevant – the financial institution it is expected to carry out
- a) a preliminary risk assessment and due diligence of the external service provider,
 - b) the agreement with the external service provider should also cover the obligation to provide information in relation to suspected fraud,
 - c) the financial institution should provide training also to external service providers on fraud prevention and management activities in accordance with point 205.

VII.5.5 Fraud prevention

218. The financial institution is expected to make every effort to prevent fraud at both strategic and operational levels.
219. The MNB expects the financial institution or group – with due regard to the principle of proportionality specified in point 10 and the self-assessment of fraud risk – to have appropriate fraud prevention procedures, technological and information security solutions and protection measure in place.
220. Fraud prevention is a set of tools, methods and programmes the purpose of which is to identify, analyse and mitigate fraud risk factors at the earliest possible stage. At the first level, prevention is represented by control processes and related audits built into business processes to reduce the risk of fraud. The MNB expects the financial institution – taking in the consideration the principle of proportionality specified in point 10 – to integrate, as part of its prevention activity, in all business processes potentially exposed to fraud the control points and in the systems supporting the respective processes the warning signals, alerts and thresholds that facilitate the detection or potential prevention of fraud attempts in due course or the minimisation of the damage caused.
221. The financial institution is expected to design and regulate its business processes – with the involvement of a competence centre, organisational unit or control function specified in point 216 – in a way that ensures the detection of potential or actual frauds as early as possible. In connection with this, the MNB also expects the financial institution – in line with the relevant statutory provisions and other related supervisory requirements⁶⁰ – to use, where possible, technological and technical procedures that enforce fraud prevention and the protection of the financial institution against fraud.

⁶⁰ MNB recommendation No 8/2020 (VI. 22.)

222. The MNB expects financial institutions to apply enhanced protective measures to prevent fraud related to the application for and use of new systems, interfaces and services by customers (e.g. registration and activity performed by misleading customers or on behalf of customers).
223. With a view to preventing frauds, the MNB expects the financial institution to
- a) define the criteria that to help detect suspected fraud, manage fraud risks and the early warning signs,
 - b) implement appropriate activity logging and monitoring as well as alerting practices,
 - c) analyse regularly its databases that facilitate the identification of fraud risks (e.g. NPL portfolio, complaints register, analysis of the quality of the branch or agent portfolio),
 - d) survey the fraud risks of new or modified products or processes,
 - e) ensure feedback from the assessment of the investigated suspected fraud incidents,
 - f) initiate process improvement measures or system improvements where necessary.
224. In connection with fraud prevention, in addition to raising and maintaining employees' awareness of the risk of fraud, it is also of particular importance to raise customers' awareness of fraud risk. Information is the primary means that a financial institution can use in respect of prospective or actual customers, for example by regularly issuing warnings of identified and typical fraud incidents, methods of deception and ways to avoid them, on the website of the financial institution, through other electronic channels (Netbank, mobile bank, Telebank, SMS) or in any other manner, and by conducting campaigns.

VII.5.6 Discovering and detecting fraud

225. The financial institution is expected to record in advance criteria and factors (red flags, early warning signs) that trigger the initiation of an investigation of a suspected fraudulent event or activity. In connection with this, the financial institution is expected to ensure that the respective employees are aware of these characteristics and factors and that appropriate tools are available to report suspected fraud.
226. With a view to preventing frauds or mitigating the impact of realised frauds – minimising the damage caused and preventing additional loss – the MNB expects the financial institutions to design its channels for reporting suspected fraud in way that provides a connection between the person detecting fraud and the person responsible for surveying, investigating or preventing it, allowing rapid communication with minimal loss of information.
227. The MNB also expects the financial institution to analyse and continuously monitor the portfolios of the financial institution and group according to a set of criteria focusing on

specific fraud risks, where it regards it as good practice to develop and apply fraud scorecards and automatic filtering.

228. With a view to preventing the future occurrence of fraud and detecting it in a timely manner, the MNB expects the financial institution to review and assess regularly the effectiveness of the methodologies, automated filtering mechanisms and monitoring systems developed for the detection and identification of frauds and, if necessary, to take steps to eliminate the shortcomings identified and to make any changes for the fine-tuning of the methodologies, automated filtering mechanisms and monitoring systems used.

VII.5.7 Investigation of suspected fraud and measures to be taken

229. With a view to preventing frauds and mitigating the impacts of realised frauds – minimising the damages caused and preventing further losses – the MNB expects the financial institution to have procedures and processes (contacting customers, stopping transactions, restriction of access) and technical tools (hardware, software and security technology) in place that facilitate the investigation of suspected frauds and the implementation of the necessary measures proportionate to the risks within the shortest possible time, commensurate with the risks, following detection of attempted fraud.
230. The MNB expects the financial institution to investigate suspected fraudulent events with the priority, deadline, focus and depth appropriate to the risk characteristics of the incident, including a quantitative and qualitative assessment of the potential and actual damage, and a detailed, objective and impartial evaluation of the facts. The investigation process is expected to include a factual investigation of the circumstances of the perpetration, the identification of the method of perpetration and the identity of the perpetrator where possible, and the identification of any weaknesses in business processes and control systems that may have led to the suspected fraud.
231. The financial institution is expected to document suspected fraud incidents in full, recording
- a) the facts and information identified during the investigation of the suspected fraud,
 - b) any weaknesses in business processes and control systems identified in relation to the suspected fraud,
 - c) the measures taken in relation to the incident, the persons responsible for implementation and the deadline of implementation, and
 - d) feedback and reporting requirements regarding the measures.
232. The MNB regards it as good practice to take decisions on the necessary measures at committee level for a pre-defined set of suspected fraud events. It is regarded as good practice to include in the committee representatives from the business or other areas directly affected by the suspected fraud, the governing body, members of other committees

(e.g. risk management committee) and representative of areas with internal control functions.

233. It should be specified in which cases the financial institution will initiate criminal proceedings in connection with suspected fraud. The MNB regards it as good practice to do so in all cases where a financial institution has identified a suspected fraudulent event, in addition to the mandatory cases prescribed by the relevant statutory provisions.
234. When collecting data on losses from operational risks, the financial institution is expected to record frauds occurred – over the limit specified by the financial institution – or failed, with tangible impact on the accounting records, and it is recommended to record also frauds occurred – over the limit specified by the financial institution – or failed, without a direct impact on the profit or loss and capital.

VII.5.8 Internal fraud

235. In view of the high risk, the financial institution is expected to pay special attention to and to manage suspected fraud incidents committed by executive board members and employees (hereinafter: internal fraud) within the framework of a special set of rules.
236. Fraud prevention and management aspects are expected to be integrated into the practices of selecting board members and employees. In connection with this, the MNB regards it as good practice to request reference letters from previous employers for certain jobs, considering the provisions of Act I of 2012 on the Labour Code.
237. The financial institution is expected to identify the activities, processes and procedures of the financial institution or group (e.g. manual posting to customer accounts, modification of contact information) that pose a significant risk of internal fraud. The financial institution is expected to reduce and restrict the use of these, or operate them under enhanced control and monitoring requirements.
238. The MNB expects the financial institution to operate a monitoring system concerning the activities performed by employees and executive board members in the financial institution's systems and the use of services provided by the financial institution or group. This should identify and analyse, among other things, events at unusual times and extraordinary transactions. With a view to reducing the risk of fraud further, the operation of the monitoring systems should be automated – subject to reviewing the parameters at least annually – and the results obtained should be analysed and evaluated by a dedicated team.

239. In order to ensure the detection of hidden internal frauds, the MNB expects – subject to complying with the relevant requirements of the labour code – the financial institution to define the range of those employees of the financial institution – subject to defining the justified exceptions –, including also the board members with governance functions, who should be exempted from work for at least 14 consecutive day once per calendar year. As a general principle, it should be prescribed that employees and, where applicable, board members with governance function, must not use the systems of the financial institution during their leave or other lawful absence (e.g. sick leave or unpaid leave). The financial institution is also expected to specify in the regulation the possible reasons for deviating from this principle, the cases in which and the systems to which the respective employee or, where applicable, the board member with governance function may have access.

VII.5.9 Monitoring system

240. The management information system is expected to contain information related to the prevention and management of frauds.
241. In addition, the management bodies of the financial institution are required to receive comprehensive information on a regular basis – at least quarterly in the case of credit institutions with a market share of more than five percent based on balance sheet total and at least semi-annually in the case of other financial institutions – on suspected fraud events, trends and actions taken in relation to them, as well as on other significant events relating to the fraud prevention and fraud management activities of the financial institution or group.
242. Internal audit should regularly – in line with the provisions of point 169 – review the fraud exposure of the financial institution or group and its activities related to the management of fraud risk (prevention, detection and surveillance, investigation, special processes for the management of internal fraud) at least every three years.

VII.5.10 Fraud risk self-assessment

243. The MNB expects credit institutions with a market share of over five percent based on the balance sheet total to conduct a self-assessment of their exposure to fraud risk on a regular basis, at least annually, in order to identify and manage their fraud exposure efficiently. The MNB expects the self-assessment to take a comprehensive approach, involving the competence centre, organisational unit or control area defined in point 216, covering the entire organisation of the financial institution –including its executive bodies and organisational units performing internal control functions – and all activities and services.
244. The MNB regards it as good practice to use a risk matrix (map) and a measurement and management methodology based on severity and frequency estimates when assessing exposure to fraud risk under point 243. It may also be regarded as good practice for a credit

institution to apply the same methodology used in its operational risk self-assessment to identify and manage its exposure to fraud risk.

245. Based on the analysis of the results of the risk assessment, the financial institution is also expected to identify the shortcomings and weaknesses of internal processes and systems, and to define priorities for fraud prevention and fraud management activities and possible mitigation of fraud risks based on these.
246. It is expected that the management bodies of the credit institution should be informed of the results of the fraud risk self-assessment and of the action plan containing measures to address the factors, processes, activities, systems, events identified as high risk. The MNB expects that the action plan, including the responsible persons and deadlines, should be approved by the governing board of the credit institution or one of its authorised committees.
247. The MNB regards it as good practice to conduct an extraordinary review of the fraud risk self-assessment – in accordance with the criteria defined by the financial institution – upon the occurrence of a significant suspected fraud incident.

VIII. Transparency and disclosure related to internal lines of defence

248. The financial institution is expected to ensure that the strategies, policies, internal regulations, internal procedures and rules of the financial institution or group are known and understood by employees to the extent necessary for their work and level of responsibility and that they are informed of changes in a timely manner.
249. In order to ensure the greatest possible transparency of the activities and operations of financial institutions, the MNB expects financial institutions to disclose clear, authentic information relevant in terms of time and content on the structure and operation of internal lines of defence annually, facilitating the real and authentic assessment of the financial institution or group, in addition to, but in compliance with, the statutory requirements. The statutory requirements and supervisory regulatory instruments relating to disclosure specify relatively few elements related to the internal lines of defence. The MNB regards the content and structure of the topics specified in the recommendation as good practice. As regards the internal lines of defence, the disclosure should cover the following items:
- a) presentation of the organisational and group structure – legal structure, governance and operational structure, key responsibilities and reporting lines – where relevant, broken down by country,
 - b) any changes since the previous disclosure in respect of the items listed in subpoint a),
 - c) presentation of the corporate system (name of the bodies, number of members and length of mandate, number of independent members, gender composition),

implementation of governance and supervisory functions (main responsibilities of each body),

- d) presentation of the bodies and committees (name, composition),
- e) method of managing conflicts of interest,
- f) description of the organisational arrangements for internal control functions,
- g) assessing the independence of internal control functions,
- h) description of the division of responsibilities between the different areas of the internal control function, coordination mechanisms,
- i) presentation of service continuity management.

250. The MNB regards it as good practice for all financial institutions to enforce the general disclosure requirements with regard to disclosure on the internal lines of defence prescribed by the Credit Institutions Act and by Articles 14–16 and 204 of MNB Recommendation No 7/2022 (IV. 2.) on the general requirements under the CRR.

251. The obligation to report infringements is stipulated by statutory requirements.⁶¹ The MNB also expects financial institutions to have procedures in place, built on well-documented and clear rules, ensuring that important and substantiated concerns and issues – not necessarily supported by evidence – raised by employees regarding the functioning of the internal lines of defence of the financial institution or group, or a subsystem thereof, are brought to the attention of the governing and supervisory bodies.

252. According to the MNB expectations the procedures under point 251 ensure

- a) that all employees are notified of any shortcomings detected,
- b) the possibility of reporting outside the reporting lines (e.g. directly to the area with the compliance function or to the head of internal audit),
- c) access to the anonymised notifications by the designated management body or functional area; the full anonymity of the notification process may be also permitted,
- d) in view of the relevant data protection regulations, the protection of the personal data of the whistleblower and of the natural person who is allegedly responsible for the respective shortcomings,
- e) that the notification has no negative consequences, whatsoever, on the whistleblower (e.g. discrimination, unfair treatment), even if, based on subsequent investigation, no action is taken against the person who is allegedly responsible for the shortcoming,
- f) feedback to the whistleblower that his notification was delivered to the competent body,
- g) the assessment, investigation, follow-up and recording of notifications.

⁶¹ Investment firms: Section 24/G of the Investment Services Act; credit institutions: Section 116 of the Credit Institutions Act

IX. Closing provisions

253. The recommendation is a regulatory instrument, issued in accordance with Article 13(2)i) of the Act CXXXIX of 2013 on the Magyar Nemzeti Bank, with no binding force on the supervised financial institutions. The content of the recommendation issued by the MNB expresses the statutory requirements, the principles proposed to be applied based on the MNB's law enforcement practice as well as the methods, market standards and practices.
254. In line with the general European supervisory practice, during its audit and monitoring activity the MNB monitors and assesses compliance with the recommendation by the financial institutions supervised by it.
255. The MNB highlights that financial organisations may make the contents of this recommendation part of their policies. In such case, the financial institution is entitled to indicate that the provisions of its relevant policies comply with the relevant recommendation issued by the MNB. If the financial institution wishes to incorporate only certain parts of the recommendation in its policies, it should not make reference to the recommendation as a whole or should only do so in respect of the parts taken from the recommendation.
256. The MNB expects the affected financial institutions to apply this Recommendation from 1 January 2023, except for the provisions set out in paragraph 257.
257. Point 30 of this Recommendation should be applied from 1 January 2024.
258. Recommendation No 27/2018 (XII. 10.) of the Magyar Nemzeti Bank on internal defence lines and the governance and control functions of financial institutions was repealed on 1 January 2023.

Dr György Matolcsy sgd.
Governor of the Magyar Nemzeti Bank

Documentation requirements concerning the financial institution's internal lines of defence

1. Ownership structure
2. Structure of the financial group, if relevant (legal and functional structure)
3. Composition and operation of the controlling and supervisory bodies
 - a) selection criteria, including how the requirements and expectations to ensure diversity are taken into consideration during the selection
 - b) number of members, duration of their mandate, rotation
 - c) independent members of the body
 - d) executive members of the body
 - e) non-executive members of the body
 - f) internal division of tasks, if relevant
4. Governance structure and organisation chart (with impact on the group, if relevant)
 - a) committees
 - aa) composition
 - ab) operation
 - b) executive body, if any
 - ba) composition
 - bb) operation
5. Persons in key positions
 - a) risk control manager
 - b) CRO
 - c) compliance assurance manager
 - d) internal audit manager
 - e) other key personnel
6. Operating structure, if relevant, together with its impact on the group
 - a) operating structure, business lines, distribution of powers and responsibilities
 - b) outsourcing
 - c) scope of products and services
 - d) territorial scope of the activity
 - e) freedom to provide services

- f) branches
 - g) subsidiaries, joint ventures, etc.
 - h) use of offshore centres
7. Description of the risk management framework, including the risk strategy
 8. Internal control system: description of the individual duties, including the related organisation, resources, competences and powers
 9. Management Information System
 10. Code of conduct and behaviour, if relevant, together with its impact on the group
 - a) strategic objectives and corporate values
 - b) internal codes and regulations, prevention policy
 - c) policy for the management of conflicts of interests
 - d) whistleblowing
 11. Status of the document recording the internal defence lines system
 - a) date of acceptance
 - b) date of last modification
 - c) date of last revision
 - d) confirming the approval of the document by the appropriate body

Annex 2 to MNB Decree No 12/2022 (VII. 11.)

Internal defence lines

Responsible internal

Primary defence lines

Internal control functions
Second defence lines

- risk control function
- compliance assurance function

Internal control functions
Third defence lines

- internal audit function