EBA/GL/2021/14

22 November 2021

Final report on

Guidelines on internal governance under Directive (EU) 2019/2034

Contents

Executive summary

For several years now, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct financial institutions' weak or superficial internal governance practices, including compliance with the framework to prevent money laundering and terrorist financing, as the reinforcement of internal governance arrangements is a critical issue for the sustainable growth of market-based financing.

Sound internal governance arrangements are fundamental if investment firms are to operate well as part of the financial system. Directive (EU) 2019/2034 sets out governance requirements for investment firms and, in particular, stresses the responsibility of the management body to ensure sound governance arrangements, the importance of a strong supervisory function that challenges management's decision-making and the need to establish and implement a sound risk strategy, risk appetite, risk culture and risk management framework.

To further harmonise investment firms' internal governance arrangements, processes and mechanisms within the EU, in line with the requirements introduced by Directive (EU) 2019/2034, the European Banking Authority (EBA) is mandated by Article 26(4) of Directive (EU) 2019/2034 to develop guidelines in this area. The guidelines apply to investment firms as defined in Article 4(1)(1) of Directive (EU) 2014/65 that do not meet all of the conditions for qualifying as small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033. These requirements apply regardless of the investment firms' governance structures (unitary board, dual board or other structure). However, the guidelines do not advocate or prefer any specific structure. The terms 'management body in its management function' and 'management body in its supervisory function' should be interpreted in accordance with the applicable law within each Member State.

The guidelines complete the various governance provisions in Directive (EU) 2019/2034, taking into account the principle of proportionality, by specifying the tasks, responsibilities and functioning of the management body, and the organisation of investment firms, including the need to create transparent structures that allow for the supervision of all their activities. The guidelines also specify in more detail the requirements under Directive (EU) 2019/2034 and aim to ensure the sound management of all risks. Risks need to be managed across all three lines of defence. While the business needs to manage its risks, the guidelines stress the responsibilities of the second line of defence (the independent risk management and compliance function) and also the third line of defence (the internal audit function).

The guidelines are consistent with the guidelines on internal governance for credit institutions and with international standards and, in particular, set out provisions that aim to foster a sound risk culture to be implemented by the management body, strengthening the management body's oversight of the investment firm's activities and implementing a sound risk management framework.

Background and rationale

1. Trust in the reliability of the financial system is crucial for its proper functioning and a prerequisite if it is to contribute to the economy as a whole. Consequently, effective internal governance arrangements are fundamental to the sustainable growth of market-based funding.

2. In recent years, internal governance issues have received increased attention from various international bodies[1]. Their main aim has been to correct financial institutions' weak or superficial internal governance practices, as identified during the financial crisis and during ongoing supervision by competent authorities. In addition, there has recently been a greater focus on conduct-related shortcomings and activities in offshore financial centres, and in the area of money laundering and terrorist financing.

3. In some cases, the absence of effective checks and balances within financial institutions resulted in a lack of effective oversight of management decision-making, which led to short-term and excessively risky management strategies. Weak oversight by the management body in its supervisory function has been identified as a contributing factor. The management body, both in its management function and, in particular, in its supervisory function, might not have understood the complexity of the business and the risks involved. Consequently, these bodies failed to identify and constrain excessive risk-taking in an effective manner.

4. Internal governance frameworks, including internal control mechanisms and risk management, were often not sufficiently integrated within financial institutions or groups. These functions were not regarded as a high priority, which impacted the stability of markets as a result. In many investment firms there was a lack of a uniform risk methodology and terminology, which meant that there was no holistic view of all risks. Internal control functions often lacked appropriate resources, status and/or expertise.

5. Conversely, sound internal governance practices helped some financial institutions to manage the financial crisis significantly better than others. These practices included the setting of an appropriate risk strategy and appropriate risk appetite levels, a holistic risk management framework and effective reporting lines to the management body.

6. Against this backdrop, there is a clear need to address the potentially detrimental effects of poorly designed internal governance arrangements on the sound management of risk, to ensure effective oversight by the management body, in particular in its supervisory function, to promote a sound risk culture at all levels of investment firms and to enable competent authorities to supervise and monitor the adequacy of internal governance arrangements.

[1] IOSCO/OECD

Legal basis

7. To further harmonise investment firms' internal governance arrangements, processes and mechanisms within the EU, the EBA, in cooperation with the ESMA, is mandated under Article 26(4) of Directive (EU) 2019/2034 to develop guidelines in this area.

8. Article 26 (1) of Directive (EU) 2019/2034 requires investment firms to have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility.

9. Article 28 of Directive (EU) 2019/2034 sets out requirements for the involvement of the management body in risk management and the setting up of a risk committee for investment firms.

10. In accordance with Article 25 of Directive (EU) 2019/2034 and Article 7 of Regulation (EU) 2019/2033, these guidelines apply on an individual and consolidated basis. For this purpose, parent undertakings and subsidiaries subject to Directive (EU) 2019/2034 must ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent and well integrated and that the governance arrangements on a consolidated basis are robust. In particular, it should be ensured that parent undertakings and subsidiaries subject to this Directive implement such arrangements, processes and mechanisms in their subsidiaries that are not subject to this Directive, including those established in third countries – including offshore financial centres.

11. The guidelines should be read, taking into account and without prejudice to Articles 9, 16, 23 and 24 of Directive (EU) 2014/65, the Commission Delegated Regulation (EU) 2017/5652 and the Commission Delegated Directive (EU) No 2017/593[3], in conjunction with the EBA guidelines on sound remuneration policies for investment firms, the joint EBA and ESMA guidelines on the assessment of the suitability of members of the management body and key function holders, the EBA guidelines on the supervisory review and evaluation process (SREP), the ESMA guidelines on certain aspects of the MiFID II compliance function requirements, the ESMA guidelines on product governance and the Regulatory Technical Standards on disclosures.

Rationale and objective of the guidelines

12. Internal governance includes all standards and principles concerned with setting an investment firm's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined and clearly allocated; how reporting

[2] Commission Delegated Regulation (EU) 2017/65 supplementing Directive (EU) 2014/65 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

[3] Commission Delegated Directive (EU) 2017/593 of 7 April 2016 supplementing Directive (EU) 2014/65 of the European Parliament and of the Council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits

lines are set up and what information they convey; and how the internal control framework is organised and implemented, including accounting procedures and remuneration policies. Internal governance also encompasses sound information technology systems, outsourcing arrangements and business continuity management.

13. Combating money laundering and terrorist financing is essential for maintaining the stability and integrity of the financial system. Uncovering the involvement of an investment firm in money laundering and terrorist financing might have an impact on its viability and on trust in the financial system. Together with the authorities and bodies (e.g. AML supervisors and financial intelligence units) responsible for ensuring compliance with anti-money laundering rules under Directive (EU) 2015/849, competent authorities have an important role to play in identifying and tackling weaknesses in this area. In this context, the guidelines clarify that identifying, managing and mitigating money laundering and financing of terrorism risks is part of sound internal governance arrangements and investment firms' risk management framework.

14. In the same way, investment firms should take into account environmental, social and governance (ESG) risk factors within their risk management framework.

15. The guidelines are intended to apply to all existing board structures without interfering with the general allocation of competences in accordance with national company law or advocating any particular structure. Accordingly, they should be applied irrespective of the board structure used (unitary or dual board structure or another structure) and across Member States. The management body, as defined in points (23) and (24) of Article 3(1) of Directive (EU) 2019/2034, should be understood as having management (executive) and supervisory (non-executive) functions.

16. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law.

17. In Member States where the management body delegates, partially or fully, the executive function to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform these executive functions and direct the business of the institution on the basis of that delegation should be understood as constituting the management function of the management body. For the purposes of these guidelines, any reference to the management body in its management function should be understood as also including the members of the executive body or the CEO, as defined in these guidelines, even if they have not been proposed or appointed as formal members of an investment firm's governing body or bodies under national law.

18. The management body is empowered to set the investment firm's strategy, objectives and overall direction, and oversees and monitors management decision-making. In its management function, the management body directs the investment firm. Senior management is accountable to the management body for the day-to-day running of the investment firm. In its supervisory function, the management body oversees and challenges the management function and provides appropriate advice. The oversight roles include reviewing the performance of the management function and the achievement of objectives, challenging the strategy, and monitoring and scrutinising the systems that ensure the integrity of financial information as well as the soundness and effectiveness of risk management and internal controls.

19. Taking into consideration all the existing governance structures provided for by national laws, competent authorities should ensure the effective and consistent application of the guidelines in their jurisdictions in accordance with the rationale and objectives of the guidelines themselves. For this purpose, competent authorities may clarify the governing bodies and functions to which the tasks and responsibilities set forth in the guidelines pertain, where this is appropriate to ensure the proper application of the guidelines in accordance with the governance structures provided for under national company law.

20. Having independent directors within the supervisory function of the management body helps to ensure that the interests of all internal and external stakeholders are considered and that independent judgement is exercised where there is an actual or potential conflict of interest[4].

21. With regard to the composition of committees and in particular with regard to independent members, the guidelines take into account the principle of proportionality. Simpler provisions have therefore been introduced for smaller investment firms.

22. While not subject to the governance requirements in accordance with Article 25 of Directive (EU) 2019/2034, small and non - interconnected investment firms should have robust strategies, policies, processes and systems in place for the identification, measurement, management and monitoring of material sources and effects of risk to clients and any material impact on own funds, material sources and effects of risk to market and any material impact on own funds and liquidity risk over an appropriate set of time horizons, including intra - day, so as to ensure that the investment firm maintains adequate levels of liquid resources in accordance with Article 29(3) of Directive (EU) 2019/2034.

23. The guidelines are consistent with the 'three lines of defence' model in identifying the functions within investment firms responsible for addressing and managing risks. Investment firms should establish and maintain a permanent and effective compliance function that operates independently from the business it controls and, where appropriate and taking into account the application of the proportionality principle, establish and maintain risk management and internal audit functions that operate independently. Where those functions

[4] In this regard, the guidelines are based on the Commission Recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board.

are not established, investment firms should ensure that the policies and procedures that they have adopted and implemented regarding risk management and internal audit achieve the same objectives.

24. The business lines, as part of the first line of defence, take risks and are directly and permanently responsible for their operational management. For that purpose, business lines should have appropriate processes and controls in place that aim to ensure risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the investment firms' risk appetite, and that the business activities are in compliance with external and internal requirements.

25. Not only business lines, but also other functions or units, e.g. HR, legal or information technology, are responsible for managing their risks and having appropriate controls in place. Other functions or units are mainly exposed to operational and reputational risks that must be considered by the compliance function and risk management function when forming an enterprise-wide holistic view of all risks. All other functions or units should also be subject to monitoring and oversight by the independent risk management function, where established, and by the compliance function as part of a risk-based approach.

26. The independent risk management function, where established, and the compliance function form the second line of defence. The risk management function facilitates the implementation of a sound risk management framework throughout the investment firm and is responsible for further identifying, monitoring, analysing, measuring, managing and reporting risks and forming a holistic view of all risks on an individual and, where applicable, consolidated basis. It challenges and assists in the implementation of risk management measures by the business lines in order to ensure that the processes and controls in place in the first line of defence are properly designed and effective. The compliance function monitors compliance with legal requirements and internal policies, provides advice on compliance issues to the management body and other relevant staff, and establishes policies and processes to manage compliance risks and to ensure compliance[5]. The compliance function and, where established, the risk management function intervene as necessary to ensure the modification of internal control and risk management systems within the first line of defence.

27. The internal audit function, where established as an independent third line of defence, conducts risk-based and general audits and reviews the internal governance arrangements, processes and mechanisms to ascertain that they are sound and effective, implemented and consistently applied. The internal audit function is also in charge of the independent review of the first two lines of defence including other internal functions, units and business lines. Investment firms that do not establish an independent audit function must establish other appropriate audit policies and procedures. In any case, the ultimate responsibility for audits remains with the management body.

28. To ensure their proper functioning, all internal control functions need to perform their tasks independently, have the appropriate financial and human resources and report directly to the

[5] See also ESMA Guidelines on certain aspects of the MiFID II compliance function requirements

management body. Within all three lines of defence, appropriate internal control procedures, mechanisms and processes should be designed, developed, maintained and evaluated under the ultimate responsibility of the management body.

29. The requirements on governance arrangements under the IFD are very similar to the requirements under the CRD and apply to investment firms, unless they meet all of the conditions to qualify as small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033 (IFR) or are subject to the CRD requirements in accordance with Article 2(2) IFD.

30. The CRD and IFD are both based on the same governance concepts and principles of good governance arrangements, while taking into account that investment firms are often smaller or less complex. Therefore a more proportionate approach is taken for such investment firms, in particular regarding the establishment of committees and control functions. Most investment firms that are now subject to the governance provisions under the IFD have been subject to the requirements under the CRD, and consistency should therefore be ensured to the extent possible to reduce the implementation costs for such firms and to ensure that consistent group-wide policies can be applied.

31. The guidelines and the principle of proportionality cannot change the minimum requirements included in the IFD. The same holds true with regard to the requirements under MiFID that apply to all investment firms. All provisions within the guidelines are subject to the principle of proportionality, meaning that they are to be applied in a manner that is appropriate, taking into account in particular the investment firm's size, internal organisation and nature, and the complexity of its activities. However, the principle of proportionality does not mean that investment firms are permitted to not meet certain requirements, i.e. requirements cannot be waived unless the IFD explicitly allows for such waivers when the underlying conditions are met.

32. The guidelines also specify the requirements under Article 26 of Directive (EU) 2019/2034, in particular with regard to the setting up of new structures e.g. in third countries, including also in offshore financial centres. These requirements aim to increase the transparency of and reduce the risks connected with such activities. Guidelines are also provided regarding investment firms' reporting on governance arrangements, including in relation to such structures.

33. The guidelines aim to establish a sound risk culture in investment firms. Risks should be taken within a well-defined framework in line with the investment firms' risk strategy and risk appetite. This includes the establishment of and ensuring compliance with a system of limits and controls. Risks within new products[6] and business areas, but also risks that may result from changes to investment firms' products, processes and systems, are to be duly identified, assessed, appropriately managed and monitored. The risk management function and compliance function should be involved in the establishment of the applicable framework and

[6] See also ESMA Guidelines on MiFID II products governance

the approval of such changes to ensure that all material risks are taken into account and that the investment firms comply with all internal and external requirements.

34. To ensure objective decision-making, oversight and compliance with external and internal requirements, including investment firms' strategies and risk limits, investment firms should implement a conflict of interest policy and internal whistleblowing procedures.

35. In order to manage conflicts of interest, the management body should ensure that a framework for the identification and, where necessary, mitigation of conflicts of interest is in place. The investment firm, its organisational substructures, staff and shareholders hold different interests that should be considered in such a framework in order to ensure that decisions are taken objectively without the undue influence of conflicts of interest. Examples of typical sources of conflicts of interest are diverging economic interests of different parties involved, or close links between decision-makers and contractual parties.

36. The management body has the highest decision-making powers. Consequently, the identification and management of conflicts of interest of members of the management body and parties closely related to the members of the management body is a cornerstone of sound internal governance practices. Therefore, the guidelines also specify the measures that should be implemented by investment firms to prudently manage conflicts of interests that may arise from entering into transactions, including with members of the management body and their related parties. Those transactions may include loans where there is the possibility for investment firms to grant loans as ancillary services.

EBA/GL/2021/14

22 November 2021

Guidelines

on internal governance under Directive (EU) 2019/2034

1. Compliance and reporting obligations

Status of these guidelines

1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010[7]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions, including investment firms, must make every effort to comply with the guidelines.

2. The guidelines set out the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom the guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at investment firms.

Reporting requirements

3. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, a competent authority must notify the EBA as to whether it complies or intends to comply with these guidelines, or otherwise stating the reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, the competent authority will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2021/14'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authority. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation (EU) No 1093/2010.

[7] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12)

2. Subject matter, scope and definitions

Subject matter

5. These guidelines specify, in accordance with Article 26(4) of Directive (EU) 2019/2034[8], the internal governance arrangements, processes and mechanisms that investment firms should implement in accordance with Title IV, Chapter 2, Section 2 of that Directive to ensure their effective and prudent management.

6. The guidelines apply without prejudice to the provisions set out in in Articles 9, 16, 23 and 24 of Directive (EU) 2014/65, in the Commission Delegated Regulation (EU) 2017/565 and in the Commission Delegated Directive (EU) 2017/593.

Addressees

7. These guidelines are addressed to competent authorities as referred to in Article 4(2), point (viii) of Regulation (EU) 1093/2010 and defined in Article 3(1), point 5 of Directive (EU) 2019/2034, and to financial institutions as referred to in Article 4(1) of Regulation (EU) 1093/2010 that are investment firms as defined in Article 4(1)(1) of Directive (EU) 2014/65, that do not fall under Article 2(2) of Directive (EU) 2019/2034 and do not meet all of the conditions to qualify as small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033.

Scope of application

8. These guidelines apply in relation to investment firms' governance arrangements as required under Directive (EU) 2019/2034, including their organisational structure and the corresponding lines of responsibility, and also to the processes to identify, manage, monitor and report all risks[9] that they are or might be exposed to, and to the internal control framework.

9. These guidelines apply on an individual and consolidated basis within the scope of application set out in accordance with Article 25 of Directive (EU) 2019/2034.

10. The guidelines intend to embrace all existing board structures and do not advocate any particular structure. The guidelines do not interfere with the general allocation of competences in accordance with national company law. Accordingly, they should be applied

[8] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU

[9] Any reference to risks in these guidelines should include all risks to which investment firms are or may be exposed, including risks to clients, risks to the market, risks to the investment firm and liquidity risks, operational risks including legal and IT risks and reputational risks, ESG risks and money laundering and terrorist financing risks.

irrespective of the board structure used (unitary and/or a dual board structure and/or another structure) across Member States. The management body, as defined in Points (23) and (24) of Article 3(1) of Directive (EU) 2019/2034, should be understood as having management (executive) and supervisory (non-executive) functions[10].

11. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law. When implementing these guidelines, competent authorities should take into account their national company law and specify, where necessary, to which body or members of the management body those functions should apply.

12. In Member States where the management body delegates, partially or fully, the executive function to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform these executive functions and direct the business of the institution on the basis of that delegation should be understood as constituting the management function of the management body. For the purposes of these guidelines, any reference to the management body in its management function should be understood as also including the members of the executive body or the CEO, as defined in these guidelines, even if they have not been proposed or appointed as formal members of the investment firm's governing body or bodies under national law.

13. In Member States where some responsibilities are directly exercised by shareholders, members or owners of the investment firms instead of the management body, investment firms should ensure that such responsibilities and related decisions are in line, as far as possible, with these guidelines applicable to the management body.

14. The definitions of CEO, chief financial officer (CFO) and key function holder used in these guidelines are purely functional and are not intended to impose the appointment of those officers or the creation of such positions unless prescribed by relevant EU or national law.

Definitions

15. Unless otherwise specified, terms used and defined in Directive (EU) 2019/2034 and Regulation (EU) No 2033/2019 have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Risk appetite	means the aggregate level and types of risk that an investment firm is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.

[10] See also recital 27 of Directive 2019/2034/EU

Risk capacity	means the maximum level of risk an investment firm is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints.
Risk culture	means an investment firm's norms, attitudes and behaviours relating to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. The risk culture influences the decisions of management and employees during their day-to-day activities and has an impact on the risks they assume.
Staff	means all employees of an investment firm and its subsidiaries on a consolidated basis and all members of their respective management bodies in their management function and their supervisory function.
Chief executive officer (CEO)	means the person who is responsible for managing and steering the overall business activities of an investment firm.
Chief financial officer (CFO)	means the person who has the overall responsibility for managing the following activities: financial resources management, financial planning and financial reporting.
Heads of internal control functions	means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance and internal audit functions.
Key function holders	means persons who have significant influence over the direction of the investment firms but who are neither members of the management body nor the CEO. They include the heads of internal control functions and the CFO, where they are not members of the management body, and, where identified on a risk-based approach by investment firms, other key function holders. Other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions.
Union parent undertaking	means a Union parent investment firm, Union parent investment holding company or Union parent mixed financial holding company that is required to abide by the prudential requirements based on the consolidated situation in accordance with Article 7 of Regulation (EU) 2019/2033.
Prudential consolidation	means the application of the prudential rules set out in Article 25 of Directive (EU) 2019/2034 and Article 7 of Regulation (EU) 2019/2033[11]

[11] Please refer also to the RTS on the consolidation of investment firms under Directive (EU) 2019/2034

Listed investment firms	means investment firms whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under points (21) and (22) of Article 4 of Directive 2014/65/EU, in one or more Member States[12].
Shareholder	means a person who owns shares in an investment firm or, depending on the legal form of an investment firm, other owners or members of the investment firm.
Directorship	means a position as a member of the management body of an investment firm or another legal entity.

3. Implementation

Date of application

16. These guidelines apply from 30 April 2022.

[12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349)

4. Guidelines

Title I – proportionality

17. Where applying these guidelines, competent authorities and investment firms should have regard to the principle of proportionality as set out in Article 26(3) of Directive (EU) 2019/2034 and specified further in Title I of these guidelines with a view to ensuring that the internal governance arrangements established by investment firms, including within the context of investment firm groups, are consistent with the individual risk profile of the firm and the group, commensurate with their size and internal organisation, relevant to their business model, suitable for the nature, scale and complexity of their activities and sufficient to effectively achieve the objectives of the relevant regulatory requirements and provisions.

18. For the purposes of the previous paragraph, account should be taken of the variety of different business models under which investment firms and investment firm groups operate, indicatively as investment advisors, portfolio managers, trading venues, custodians, execution or wholesale brokers, trading firms, and others. Accordingly, for the internal governance arrangements to be deemed to be consistent with the individual risk profile of the firm and the group, commensurate with their size and internal organisation, relevant to their business model, suitable for the nature, scale and complexity of their activities and sufficient to effectively achieve the objectives of the relevant regulatory requirements and provisions, it should be ensured that investment firms with a more complex organisation or with a larger scale should have more sophisticated governance arrangements, while investment firms with a simpler organisation or with a smaller scale may implement simpler governance arrangements. Investment firms should, however, note that the size or systemic importance of an investment firm may not, in itself, be indicative of the extent to which an investment firm is exposed to risks.

19. Where applying the principle of proportionality as set out in Article 26 (3) of Directive (EU) 2019/2034 and specified further in paragraph 20 of these guidelines, competent authorities and investment firms should ensure that such application does not result in the regulatory requirements being waived for investment firms or being applied in a way that means robust governance arrangements, a clear organisational structure, adequate internal control mechanisms, sound and effective risk management and appropriate remuneration policies are not ensured.

20. For the purpose of the application of the principle of proportionality and in order to ensure the appropriate implementation of the regulatory requirements and of these guidelines, the following aspects should be taken into account by investment firms and competent authorities:

a. the size in terms of the balance sheet of the investment firm and its subsidiaries within the scope of prudential consolidation;

b. whether the value of the investment firm's on and off-balance sheet assets is on average equal to or less than EUR 100 million over the four-year period immediately preceding the given financial year in accordance with the criteria set out in point (a) of Article 32(4) of Directive (EU) 2019/2034;

c. the assets under management;

d. whether the investment firm is authorised to hold client money or assets;

e. the assets safeguarded and administered;

f. the volume of client orders handled;

g. the volume of daily trading flows;

h. the geographical presence of the investment firm and the size of its operations in each jurisdiction, including in third-country jurisdictions;

i. the legal form of the investment firm, including whether the investment firm is part of a group and, if so, the proportionality assessment for the group;

j. whether it is a listed investment firm;

k. whether the investment firm is authorised to use internal models for the measurement of capital requirements (e.g. the Internal Ratings Based Approach);

l. the type of authorised activities, the services performed by the investment firm (e.g. Sections A and B of Annex I to Directive 2014/65/EU) and other services (e.g. clearing services) performed by the investment firm;

m. the underlying business model and strategy; the nature and complexity of the business activities, and the investment firm's organisational structure;

n. the risk strategy, risk appetite and actual risk profile of the investment firm, also taking into account the result of the SREP capital and SREP liquidity assessments;

o. the ownership and funding structure of the investment firm;

p. the type of clients;

q. the complexity of the financial instruments or contracts;

r. the outsourced functions and distribution channels; and

s. the existing information technology (IT) systems, including business continuity systems and outsourced functions in this area.

21. Investment firms that are legal persons managed by a single natural person should have alternative arrangements in place which ensure the sound and prudent management of such investment firms and the adequate consideration of internal governance arrangements.

Title II – role and composition of the management body and committees

1 Role and responsibilities of the management body

22. The management body must have ultimate and overall responsibility for the investment firm and defines, oversees and is accountable for the implementation of the governance arrangements as referred to in particular under Articles 26, 28 and 29 of Directive (EU) 2019/2034, within the investment firm that ensure the effective and prudent management of the investment firm.

23. The duties of the management body should be clearly defined, distinguishing between the duties of the management (executive) function and of the supervisory (non-executive) function. The responsibilities and duties of the management body should be described in a written document and duly approved by the management body. All members of the management body should be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees, where appropriate.

24. The management body in its supervisory function and its management function should interact effectively. Both functions should provide each other with sufficient information to allow them to perform their respective roles. In order to have appropriate checks and balances in place, decision-making within the management body should not be dominated by a single member or a small subset of its members.

25. Without prejudice to the tasks and responsibilities assigned to the management body under Directive (EU) 2014/65, the management body's responsibilities should include setting, approving and overseeing the implementation of:

a. the overall business strategy and the key policies of the investment firm within the applicable legal and regulatory framework, taking into account the investment firm's long-term financial interests and solvency;

b. the overall risk strategy, including the investment firm's risk appetite and its risk management framework, including adequate policies and procedures, taking into

account the macroeconomic environment and the business cycle of the investment firm and measures to ensure that the management body devotes sufficient time to risk management issues; an adequate and effective internal governance and internal control framework that includes a clear organisational structure and well-functioning internal control mechanisms. Such mechanisms should include a permanent and effective compliance function and, where appropriate and proportionate in accordance with Title I, internal risk management and internal audit functions that have sufficient authority, stature and resources to perform their functions independently, and ensure compliance with applicable regulatory requirements in the context of the prevention of money laundering and terrorism financing; and also targets for the liquidity management of the investment firm;

c. a remuneration policy that is in line with the remuneration principles set out in Articles 26 and 30 to 33 of Directive (EU) 2019/2034 and the EBA guidelines on sound remuneration policies under Directive (EU) 2019/2034[13];

d. arrangements that aim to ensure that the individual and collective suitability assessments of the management body are carried out effectively, that the composition and succession planning of the management body are appropriate, and that the management body performs its functions effectively[14];

e. a selection and suitability assessment process for key function holders[15];

f. arrangements that aim to ensure the internal functioning of each committee of the management body, where established, detailing the:

    i. role, composition and tasks of each of them;

    ii. appropriate information flows, including the documentation of recommendations and conclusions, and reporting lines between each committee and the management body, competent authorities and other parties;

g. a risk culture in line with Section 8 of these guidelines that addresses the investment firm's risk awareness and risk-taking behaviour;

h. a corporate culture and values in line with Section 9 that foster responsible and ethical behaviour, including a code of conduct or similar instrument;

[13] EBA guidelines on sound remuneration policies under the IFD

[14] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders.

[15] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders.

i. a conflict of interest policy at the investment firm level in line with Section 10; and for staff in line with Section 11; and

j. arrangements that aim to ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards.

26. When setting up, approving and overseeing the implementation of the aspects listed in paragraph 25, the management body should aim to ensure a business model and governance arrangements – including a risk management framework – that take into account the risks investment firms are or might be exposed to or the risks that they pose or might pose to others[16]. When taking into account all risks, investment firms should take into account all relevant risk factors, including environmental, social and governance risks factors. Investment firms should consider that the latter may drive their prudential risks[17]. Such ESG risk factors include, e.g. legal risks in the area of contractual or labour law, risks relating to potential human rights violations or other ESG risk factors that may affect the country where a service provider is located and its ability to provide the agreed service levels.

27. The management body should oversee the process of disclosure and communications with external stakeholders and competent authorities.

28. All members of the management body should be informed about the overall activity, financial and risk situation of the investment firm, taking into account the economic environment, and also about any decisions taken that have a major impact on the investment firm's business.

29. A member of the management body may be responsible for an internal control function as referred to in Title V, Section 18.1, provided that the member does not have other mandates that would compromise the member's internal control activities and the independence of the internal control function.

30. The management body should monitor, periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies relating to the responsibilities listed in paragraphs 25 and 26. The internal governance framework and its implementation should be reviewed and updated on a periodic basis, taking into account the proportionality principle, as further explained in Title I. A deeper review should be carried out where material changes affect the investment firm.

31. Where investment firms are legal persons managed by a single natural person in accordance with their constitutive rules and national laws, the references in these guidelines to a management body should be construed as applying to the single person that is responsible for

[16] See Article 26 of Directive (EU) 2019/2034.

[17] See EBA discussion paper on ESG risk management and supervision published under the CRD Art. 98(8) for a description of the EBA's understanding of ESG risks, transmission channels and recommendations for arrangements, processes, mechanisms and strategies to be implemented by institutions to identify, assess and manage ESG risks.

implementing alternative arrangements to ensure the sound and prudent management of such an investment firm and the adequate consideration of internal governance arrangements.

2 Management function of the management body

32. In its management function, the management body should actively engage in the business of an investment firm and should take decisions on a sound and well-informed basis.

33. In its management function, the management body should be responsible for the implementation of the strategies set out by the management body and regularly discuss the implementation and appropriateness of these strategies with the management body in its supervisory function. The operational implementation may be carried out by the investment firm's management.

34. In its management function, the management body should constructively challenge and critically review propositions, explanations and information received when exercising its judgement and taking decisions. In its management function, the management body should comprehensively report to, and inform regularly and where necessary without undue delay, the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the investment firm, e.g. material decisions on business activities and risks taken, the evaluation of the investment firm's economic and business environment, liquidity and sound capital base, and assessment of its material risk exposures.

35. Without prejudice to the national transposition of Directive (EU) 2015/849 Anti-Money Laundering Directive (AMLD), the management body should identify one of its members in line with the requirements under Article 46(4) of Directive (EU) 2015/849 to be responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this directive, including the corresponding AML/CFT policies and procedures in the institution and at the level of the management body .

3 Supervisory function of the management body

36. The role of the members of the management body in its supervisory function should include monitoring and constructively challenging the strategy of the investment firm.

37. Without prejudice to national law, in its supervisory function the management body should include independent members as provided for in Section 9.3 of the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive (EU) 2013/36 and Directive (EU) 2014/65.

38. Without prejudice to the responsibilities assigned under the applicable national company law, in its supervisory function the management body should:

a. oversee and monitor management decision-making and actions and provide effective oversight of the management body in its management function, including monitoring and scrutinising its individual and collective performance and the implementation of the investment firm's strategy and objectives;

b. constructively challenge and critically review proposals and information provided by members of the management body in its management function, as well as its decisions;

c. appropriately fulfil the duties and role of the risk committee and the remuneration committee, where no such committees have been set up;

d. ensure and periodically assess the effectiveness of the investment firm's internal governance framework and take appropriate steps to address any identified deficiencies;

e. oversee and monitor that the investment firm's strategic objectives, organisational structure and risk strategy, its risk appetite and risk management framework, as well as other policies (e.g. remuneration policy) and the disclosure framework are implemented consistently;

f. monitor that the risk culture of the investment firm is implemented consistently;

g. oversee the implementation and maintenance of a code of conduct or similar code and effective policies to identify, manage and mitigate actual and potential conflicts of interest;

h. oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework;

i. ensure that the heads of internal control functions are able to act independently and, regardless of the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments affect or may affect the investment firm; and

j. monitor the implementation of the internal audit plan following the prior involvement of the risk committee, where established.

4 Role of the chair of the management body

39. The chair of the management body should lead the management body, contribute to an efficient flow of information within the management body and between the management body and its committees, where established, and should be responsible for its effective overall functioning.

40. The chair should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.

41. Where the chair is permitted to assume executive duties, the investment firm should have measures in place to mitigate any adverse impact on the investment firm's checks and balances (e.g. by designating a lead board member or a senior independent board member, or by having a larger number of non-executive members within the management body in its supervisory function). The chair of the management body in its supervisory function at an investment firm must not simultaneously exercise the functions of a CEO within the same investment firm, unless justified by the investment firm and authorised by competent authorities.

42. The chair should set meeting agendas and ensure that strategic issues are discussed as a priority. He or she should ensure that decisions of the management body are taken on a sound and well-informed basis and that documents and information are received in enough time before the meeting.

43. The chair of the management body should contribute to a clear allocation of duties between members of the management body and the existence of an efficient flow of information between them in order to allow the members of the management body in its supervisory function to constructively contribute to discussions and to cast their votes on a sound and well-informed basis.

5 Committees of the management body in its supervisory function

5.1 Setting up committees

44. In accordance with Article 28 of the IFD and unless otherwise specified by national law,[18] investment firms where the value of their on and off-balance sheet assets is on average more than EUR 100 million over the four-year period immediately preceding the given financial year must establish risk and remuneration committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body.

45. Where no risk committee is established, the references in these guidelines to this committee should be construed as referring to the management body in its supervisory function.

46. Investment firms may, taking into account the criteria set out in Title I of these guidelines, establish other committees (e.g. anti-money laundering/counter terrorist financing (AML/CTF), ethics, conduct and compliance committees).

[18] Article 28 of Directive (EU) 2019/2034 requires investment firms that do not meet the criteria set out in point (a) of Article 32(4) to establish a risk committee composed of members of the management body who do not perform any executive function in the investment firm concerned.

47. Investment firms should ensure a clear allocation and distribution of duties and tasks between specialised committees of the management body. Each committee should have a documented mandate, including the scope of its responsibilities, by the management body in its supervisory function and establish appropriate working procedures.

48. Committees should support the supervisory function in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees should not in any way release the management body in its supervisory function from collectively fulfilling its duties and responsibilities.

5.2 Composition of committees[19]

49. All committees should be chaired by a non-executive member of the management body who is able to exercise objective judgement.

50. Independent members[20] of the management body in its supervisory function should be actively involved in committees.

51. Where committees have to be set up in accordance with Directive (EU) 2019/2034 or national law, as a general principle they should be composed as a general principle of at least three members and have at least one independent member, taking into account the criteria set out in Title I of these guidelines and the joint EBA and ESMA guidelines on the assessment of the suitability of members of the management body and key function holders. Where there is not a sufficient number of members within the management body in its supervisory function to ensure a sound composition of committees as set out in this section, the tasks of the committee may be delegated to one member of the management body in its supervisory function, who is supported as appropriate by staff. Committees may be composed of the same group of members, taking into account the criteria set out in Title I and the number of independent members of the management body in its supervisory function alongside the specific experience, knowledge and skills that are individually or collectively required for the committees. The reasoning for the composition of committees should be documented.

52. The risk committee should be composed of non-executive members of the management body in its supervisory function of the investment firm concerned. The remuneration committee should be composed in accordance with Section 2.3 of the EBA guidelines on sound remuneration policies[21].

53. The risk committee should be chaired, where possible, by an independent member. Members of the risk committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning, respectively, the selection process and suitability requirements as well as risk management and control practices. In all investment firms, the chair of the risk

[19] This section should be read in conjunction with the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive (EU) 2013/36 and Directive (EU) 2014/65.

[20] As defined in Section 9.3 of the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive (EU) 2013/36 and Directive (EU) 2014/65

[21] EBA guidelines on sound remuneration policies under Article 34 (3) of Directive (EU) 2019/2034

committee should, where possible, neither be the chair of the management body nor the chair of any other committee.

5.3 Committees' processes

54. Committees should regularly report to the management body in its supervisory function.

55. Committees should interact with each other as appropriate. Without prejudice to paragraph 51, such interaction could take the form of cross-participation, so that the chair or a member of a committee may also be a member of another committee.

56. Members of committees should engage in open and critical discussions, during which dissenting views are discussed in a constructive manner.

57. Committees should document the agendas of committee meetings and their main results and conclusions.

58. The risk committee should at least:

    a. have access to all the relevant information and data necessary to perform its role, including information and data from relevant corporate and control functions (e.g. legal, finance, human resources, IT, internal audit, risk and compliance, including information on AML/CTF compliance and aggregated information on suspicious transaction reports, and ML/TF risk factors);

    b. receive regular reports, ad hoc information, communications and opinions from heads of internal control functions concerning the current risk profile of the investment firm, its risk culture and its risk limits, as well as on any material breaches[22] that may have occurred, with detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them; periodically review and decide on the content, format and frequency of the information regarding risk to be reported to it; and

    c. where necessary, ensure the proper involvement of the internal control functions and other relevant functions (human resources, legal and finance) within their respective areas of expertise and/or seek external expert advice.

5.4 Role of the risk committee

59. Where established, the risk committee should at least:

[22] With regard to serious breaches in the area of AML/TF, please refer also to the guidelines to be issued under Article 117 (6) of Directive 2013/36/EU, specifying the manner of cooperation and information exchange between the authorities referred to in paragraph 5 of this Article, particularly in relation to cross-border groups and in the context of identifying serious breaches of anti-money laundering rules.

a. advise and support the management body in its supervisory function with regard to the investment firm's overall current and future risk strategy and risk appetite, and assist the management body in overseeing the implementation of that strategy, to ensure that they are in line with the business objectives, corporate culture and values of the investment firm;

b. assist the management body in its supervisory function in overseeing the implementation of the investment firm's risk strategy and setting the corresponding limits;

c. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of an investment firm, such as risks to clients, risks to the market, risks to firms, operational risk (including legal and IT risks) and reputational risk in order to assess their adequacy against the approved risk strategy and risk appetite;

d. provide the management body in its supervisory function with recommendations for necessary adjustments to the risk strategy resulting from, inter alia, changes to the business model of the investment firm, market developments or recommendations made by the risk management function;

e. provide advice on the appointment of external consultants that the supervisory function may decide to engage for advice or support;

f. review a number of possible scenarios, including stressed scenarios, to assess how the investment firm's risk profile would react to external and internal events;

g. oversee the alignment between all material financial instruments and services offered to clients and the business model and risk strategy of the investment firm. The risk committee, where established, should assess the risks associated with the financial instruments and services offered and take into account the alignment between the prices assigned to and the profits gained from those products and services; and

h. assess the recommendations of internal or external auditors and follow up on the appropriate implementation of measures taken.

60. The risk committee should collaborate with other committees whose activities may have an impact on the risk strategy (e.g. the remuneration committee, where established) and regularly communicate with the investment firm's internal control functions, in particular the risk management function.

Title III – governance framework

6 Organisational framework and structure

6.1 Organisational framework

61. The management body of an investment firm should ensure a suitable and transparent organisational and operational structure for that investment firm and should have a written description of it. The structure should promote and demonstrate the effective and prudent management of an investment firm at the individual and consolidated levels.

62. The management body should ensure that the internal control functions have the appropriate financial and human resources as well as powers to effectively perform their role. As a minimum, the compliance function should operate independently, including that there is an appropriate segregation of duties. The reporting lines and the allocation of responsibilities, in particular among key function holders, within an investment firm should be clear, well-defined, coherent, enforceable and duly documented. The documentation should be updated as appropriate.

63. The structure of the investment firm should not impede the ability of the management body to oversee and manage effectively the risks the investment firm or the group faces or the ability of the competent authority to effectively supervise the investment firm.

64. The management body should assess whether and how material changes to the group's structure (e.g. setting up of new subsidiaries, mergers and acquisitions, selling or winding-up parts of the group, or external developments) impact on the soundness of the investment firm's organisational framework. Where weaknesses are identified, the management body should make any necessary adjustments swiftly.

6.2 Know your structure

65. The management body should fully know and understand the legal, organisational and operational structure of the investment firm ('know your structure') and ensure that it is in line with its approved business and risk strategy and risk appetite and covered by its risk management framework

66. The management body should be responsible for the approval of sound strategies and policies for the establishment of new structures. Where an investment firm creates many legal entities within its group, their number and, in particular, the interconnections and transactions between them should not pose challenges for the design of its internal governance, nor for the effective management and oversight of the risks of the group as a whole. The management body should ensure that the structure of an investment firm and, where applicable, the structures within a group, taking into account the criteria specified in Section 7, are clear, efficient and transparent to the investment firm's staff, shareholders and other stakeholders and to the competent authority.

67. The management body should guide the investment firm's structure, its evolution and its limitations and should ensure that the structure is justified and efficient and does not involve undue or inappropriate complexity.

68. The management body of a Union parent undertaking should understand not only the legal, organisational and operational structure of the group, but also the purpose and activities of its different entities and the links and relationships among them. This includes understanding group-specific operational risks and intra-group exposures as well as how the group's funding, capital, liquidity and risk profiles could be affected under normal and adverse circumstances. The management body should ensure that the parent investment firm is able to produce information on the group in a timely manner regarding the type, characteristics, organisational chart, ownership structure and businesses of each legal entity, and that the investment firms within the group comply with all the supervisory reporting requirements on an individual and consolidated basis.

69. The management body of a Union parent undertaking should ensure that the different group entities (including the Union parent undertaking itself) receive enough information to have a clear understanding of the general objectives, strategies and risk profile of the group and how the group entity concerned is embedded into the group's structure and operational functioning. Such information – and any revisions thereof – should be documented and made available to the relevant functions concerned, including the management body, business lines and internal control functions. The members of the management body of a Union parent undertaking should keep themselves informed about the risks the group's structure causes, taking into account the criteria specified in Section 7 of the guidelines. This includes receiving:

    a. information on major risk drivers;

    b. regular reports assessing the investment firm's overall structure and evaluating the compliance of individual entities' activities with the approved group-wide strategy; and

    c. regular reports on topics where the regulatory framework requires compliance at the individual and consolidated levels.

6.3 Complex structures and non-standard or non-transparent activities

70. Investment firms should avoid setting up complex and potentially non-transparent structures. Investment firms should take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering, terrorist financing or other financial crimes and the

respective controls and legal framework in place[23]. To this end, investment firms should take into account, as a minimum:

a. the extent to which the jurisdiction in which the structure will be set up complies effectively with EU and international standards on tax transparency, anti-money laundering and countering the financing of terrorism[24];

b. the extent to which the structure serves an obvious economic and lawful purpose;

c. the extent to which the structure could be used to hide the identity of the ultimate beneficial owner;

d. the extent to which the customer's request that leads to the possible setting-up of a structure gives rise to concern;

e. whether the structure might impede appropriate oversight by the investment firm's management body or the investment firm's ability to manage the related risk; and

f. whether the structure poses obstacles to effective supervision by competent authorities.

71. In any case, investment firms should not set up opaque or unnecessarily complex structures that have no clear economic rationale or legal purpose, or structures that could raise concerns that these might be created for a purpose connected with financial crime.

72. When setting up such structures, the management body should understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures should be approved and maintained only when their purpose has been clearly defined and understood, and when the management body is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured. The more complex and opaque the organisational and operational structure, and the greater the risks, the more intensive the oversight of the structure should be.

73. Investment firms should document their decisions and be able to justify their decisions to competent authorities.

[23] For further details on the assessment of country risk and the risk associated with individual products and customers, investment firms should also refer to the joint guidelines on ML/TF risk factors (EBA GL JC/2017/37) currently under review.

[24] See also Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

74. The management body should ensure that appropriate actions are taken to avoid or mitigate the risks of activities within such structures. This includes ensuring that:

    a. the investment firm has in place adequate policies and procedures and documented processes (e.g. applicable limits and information flows) for the consideration, compliance, approval and risk management of such activities, taking into account the consequences for the group's organisational and operational structure, its risk profile and its reputational risk;

    b. information concerning these activities and the risks thereof is accessible to the Union parent undertaking as well as internal and external auditors and is reported to the management body in its supervisory function and to the competent authority that granted authorisation; and

    c. the investment firm periodically assesses the continuing need to maintain such structures.

75. These structures and activities, including their compliance with legislation and professional standards, should be subject to a regular review. Where an internal audit function is established, it should perform the review on a risk-based approach.

76. Investment firms should take effective risk management measures when they perform non-standard or non-transparent activities for clients (e.g. helping clients to set up vehicles in offshore jurisdictions, developing complex structures, facilitating transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks. In particular, investment firms should analyse the reason why a client wants to set up a particular structure.

7 Organisational framework in a group context

77. In accordance with Article 25 of Directive (EU) 2019/2034 and Article 7 of Regulation (EU) 2019/2033, and unless Article 8 of Regulation (EU) 2019/2033 is applied by competent authorities, Union parent undertakings and their subsidiaries subject to Directive (EU) 2019/2034 should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated basis. To this end, undertakings and subsidiaries within the scope of prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries not subject to Directive (EU) 2019/2034, including those established in third countries including in offshore financial centres – to ensure robust governance arrangements on a consolidated basis. Competent functions within the Union parent undertaking and its subsidiaries should interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms should ensure that the Union parent undertaking has sufficient data and information and is able to assess the group-wide risk profile as detailed in Section 6.2.

78. The management body of a subsidiary that is subject to Directive (EU) 2019/2034 should adopt and implement at the individual level the group-wide governance policies established at the consolidated level, in a manner that complies with all the specific requirements under EU and national law.

79. At the consolidated level, the Union parent undertaking should ensure adherence to the group-wide governance policies and internal control framework as referred to in Title V by all investment firms and other entities within the scope of prudential consolidation, including its subsidiaries not themselves subject to Directive (EU) 2019/2034. When implementing governance policies, the Union parent undertaking should ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

80. A Union parent undertaking should consider the interests of all its subsidiaries, and how strategies and policies contribute to the interests of each subsidiary and the interests of the group as a whole over the long term.

81. A Union parent undertaking and its subsidiaries should ensure that the investment firms and entities within the group comply with all the specific regulatory requirements in any relevant jurisdiction.

82. The Union parent undertaking should ensure that subsidiaries established in third countries that are included in the scope of prudential consolidation have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of Articles 25 to 32 of Directive (EU) 2019/2034 and these guidelines, as long as this is not unlawful under the laws of the third country.

83. The governance requirements of Directive 2019/2034/EU and the provisions in these guidelines apply to investment firms located in the EU independent of the fact that they may be subsidiaries of a parent undertaking in a third country. Where an EU subsidiary of a parent undertaking in a third country is a Union parent undertaking, the scope of prudential consolidation within the EU does not include the level of the parent investment firm located in a third country and other direct subsidiaries of that parent undertaking. The Union parent undertaking should ensure that the group-wide governance policy of the parent investment firm in a third country is taken into consideration within its own governance policy insofar as this is not contrary to the requirements set out under relevant EU law, including Directive (EU) 2019/2034 and the additional specifications under these guidelines.

84. When establishing policies and documenting governance arrangements, investment firms should take into account the aspects listed in Annex I. While policies and documentation may be included in separate documents, investment firms should consider combining them or referring to them in a single governance framework document.

Title IV – risk culture and business conduct

8 Risk culture

85. A sound, diligent and consistent risk culture should be a key element of investment firms' effective risk management and should enable investment firms to make sound and informed decisions.

86. Investment firms should develop an integrated and investment firm-wide risk culture, based on a full understanding and holistic view of the risks they face including the risks to clients, to markets, the risk to the investment firm itself and the liquidity risks, in particular those which can have a material impact on or deplete the level of own funds available and how they are managed, taking into account the investment firm's risk capacity and risk appetite.

87. Investment firms should develop a risk culture through policies, communication and staff training regarding the investment firms' activities, strategy and risk profile, and should adapt communication and staff training to take into account staff's responsibilities regarding risk-taking and risk management.

88. Staff should be fully aware of their responsibilities relating to risk management. Risk management should not be confined to risk specialists or internal control functions. Business units, under the oversight of the management body, should be primarily responsible for managing risks on a day-to-day basis in line with the investment firm's policies, procedures and controls, taking into account the investment firm's risk appetite and risk capacity.

89. A strong risk culture should include but is not necessarily limited to:

    a. Tone from the top: the management body should be responsible for setting and communicating the investment firm's core values and expectations. The behaviour of its members should reflect these values. Investment firms' management, including key function holders, should contribute to the internal communication of core values and expectations to staff. Staff should act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the investment firm (e.g. to the competent authority through a whistleblowing process). The management body should, on an ongoing basis, promote, monitor and assess the risk culture of the investment firm, consider the impact of the risk culture on the financial stability, risk profile and robust governance of the investment firm and make changes where necessary.

    b. Accountability: relevant staff at all levels should know and understand the core values of the investment firm and, to the extent necessary for their role, its risk appetite and risk capacity. They should be capable of performing their roles and be aware that they will be held accountable for their actions in relation to the investment firm's risk-taking behaviour.

c. Effective communication and challenge: a sound risk culture should promote an environment of open communication and effective challenge in which decision-making processes encourage a broad range of views, allow for testing of current practices, stimulate a constructive critical attitude among staff and promote an environment of open and constructive engagement throughout the entire organisation.

d. Incentives: appropriate incentives should play a key role in aligning risk-taking behaviour with the investment firm's risk profile and its long-term interests[25].

9 Corporate values and code of conduct

90. The management body should develop, adopt, adhere to and promote high ethical and professional standards, taking into account the specific needs and characteristics of the investment firms, and should ensure the implementation of such standards (through a code of conduct or similar instrument). It should also oversee adherence to these standards by staff. Where applicable, the management body may adopt and implement the investment firm's group-wide standards or common standards released by associations or other relevant organisations.

91. Investment firms should ensure that there is no discrimination towards staff based on gender, race, colour, ethnic or social origin, genetic features, languages, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

92. Investment firms' policies should be gender-neutral. This includes, but is not limited to, remuneration, recruitment policies, career development and succession plans, access to training and the ability to apply for internal vacancies. Institutions should ensure equal opportunities[26] for all staff irrespective of their gender, including with regard to career perspectives, and aim to improve representation of the underrepresented gender in positions within the management body as well as in the group of staff that have managerial responsibilities as defined in the Commission's Delegated Regulation (regulatory technical standards (RTS) on identified staff). Investment firms should monitor the trend in the gender pay gap. Where investment firms have 50 or more staff[27], the monitoring should be separately for identified staff (excluding members of the management body), members of the management body in its management function, members of the management body in the supervisory function and other staff. Institutions should have policies that facilitate the reintegration of staff after maternity, paternity or parental leave.[28]

[25] Please refer also to the EBA guidelines on sound remuneration policies under Directive (EU) 2034/2019

[26] See also Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation

[27] See also EBA Guidelines on sound remuneration policies under Directive (EU) 2019/2034

[28] See also EBA Guidelines on sound remuneration policies under Directive (EU) 2019/2034

93. The standards implemented should aim to enhance the institution's robust governance arrangements and reduceing the risk to which the investment firm is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on an investment firm's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties, and the loss of brand value and consumer confidence.

94. The management body should have clear and documented policies for how these standards should be met. These policies should:

    a. remind staff that all the investment firm's activities should be conducted in compliance with the applicable law and with the investment firm's corporate values;

    b. promote risk awareness through a strong risk culture in line with Section 9 of the guidelines, conveying the management body's expectation that activities will not go beyond the defined risk appetite and limits defined by the investment firm and the respective responsibilities of staff;

    c. set out principles on and provide examples of acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime including but not limited to fraud, money laundering and terrorist financing (ML/TF), anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws, tax offences, whether committed directly or indirectly, including through unlawful or banned dividend arbitrage schemes;

    d. clarify that in addition to complying with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and

    e. ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.

95. Investment firms should monitor compliance with such standards and ensure staff awareness, e.g. by providing training. Investment firms should define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance. The results should periodically be reported to the management body.

10 Conflict of interest policy at firm level

96. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at firm level, e.g. as a result of the various activities and roles of the investment firm, of different investment firms within the scope of

prudential consolidation or of different business lines or units within an investment firm, or with regard to external stakeholders. When setting these policies, investment firms should be aware that these policies need also to be compliant with Article 16(3) and 23 of Directive 2014/65/EU and Articles 33 to 35 of the Commission delegated regulation 2017/565.

97. Investment firms' measures to manage or where appropriate mitigate conflicts of interest should be documented and include, inter alia:

    a. an appropriate segregation of duties, e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons;

    b. establishing information barriers, e.g. through the physical separation of certain business lines or units.

11 Conflict of interest policy for staff[29]

98. Without prejudice to Article 23 of Directive 2014/65/EU and Section 3 of the Chapter 2 of the Commission Delegated Regulation (EU) No 2017/565, the management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts between the interests of the investment firm and the private interests of staff, including members of the management body, which could adversely influence the performance of their duties and responsibilities. A Union parent undertaking should consider interests within a group-wide conflict of interest policy on a consolidated basis.

99. The policy should aim to identify conflicts of interest of staff, including the interests of their closest family members. Investment firms should take into consideration that conflicts of interest may arise not only from present but also from past personal or professional relationships. Where conflicts of interest arise, investment firms should assess their materiality and decide on and implement mitigating measures as appropriate.

100. Regarding conflicts of interest that may result from past relationships, investment firms should set an appropriate timeframe for which they want staff to report such conflicts of interest, on the basis that these may still have an impact on staff's behaviour and participation in decision-making.

101. The policy should cover at least the following situations or relationships where conflicts of interest may arise:

    a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property

[29] This section should be read in conjunction with the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

rights, membership of a body or ownership of a body or entity with conflicting interests);

b. personal or professional relationships with the owners of qualifying holdings in the investment firms;

c. personal or professional relationships with staff of the investment firms or entities included within the scope of prudential consolidation (e.g. family relationships);

d. other employment and previous employment within the recent past (e.g. five years);

e. personal or professional relationships with relevant external stakeholders (e.g. being associated with material suppliers, consultancies or other service providers); and

f. political influence or political relationships.

102. Notwithstanding the above, investment firms should take into consideration that being a shareholder of an investment firm or using other services of an investment firm should not lead to a situation where staff are considered to have a conflict of interest if they stay within an appropriate de minimis threshold.

103. The policy should set out the processes for reporting and communication to the function responsible under the policy. Staff should have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.

104. The policy should differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event (e.g. a transaction or the selection of a service provider, etc.) and can usually be managed with a one-off measure. In all circumstances, the interests of the investment firm should be central to the decisions taken.

105. The policy should set out procedures, measures, documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures. Such procedures, requirements, responsibilities and measures should include:

a. entrusting conflicting activities or transactions to different persons;

b. preventing staff who are also active outside the investment firm from having inappropriate influence within the investment firm regarding those other activities;

c. establishing the responsibility of the members of the management body to abstain from voting on any matter where a member has or may have a conflict of interest or

where the member's objectivity or ability to properly fulfil his or her duties to the investment firm may be otherwise compromised;

d. preventing members of the management body from holding directorships in competing investment firms.

106. The policy should specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the investment firms. Investment firms should take into consideration that conflicts of interest can have an impact on the independence of mind of members of the management body[30].

107. When mitigating identified conflicts of interest of members of the management body, investment firms should document the measures taken, including the reasoning on how such measures are effective in ensuring objective decision-making.

108. Actual or potential conflicts of interest that have been disclosed to the responsible function within the investment firm should be appropriately assessed and managed. If a conflict of interest of staff is identified, the investment firm should document the decision taken, in particular if the conflict of interest and the related risks have been accepted; and if it has been accepted, how this conflict of interest has been satisfactorily mitigated or remedied.

109. All actual and potential conflicts of interest at the management body level, individually and collectively, should be adequately documented, communicated to the management body and discussed, decided on and duly managed by the management body.

11.1 Conflicts of interest policy in the context of loans and other transactions with members of the management body and their related parties

110. As part of their conflicts of interest policies for staff (Section 11) and the management of conflicts of interest of members of the management body as set out in paragraph 107, the management body should set out a framework for identifying and managing conflicts of interest in the context of granting loans and entering into other transactions, e.g. initial public offerings, service agreements or outsourcing agreements with members of the management body and their related parties.

111. Investment firms should consider additional categories of related parties to whom they apply, in whole or in part, their conflicts of interest framework regarding loans and transactions.

[30] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

112. The conflicts of interest framework should ensure that decisions regarding loans and entering into other transactions with members of the management body and their related parties are taken objectively, without undue influence from conflicts of interest and are, as a general principle, conducted at arm's length.

113. The management body should set out the applicable decision-making processes for granting loans and entering into other transactions with members of the management body and their related parties. This framework may provide for a differentiation between standard business transactions[31] entered into in the ordinary course of business and concluded on normal market terms and staff transactions, which are concluded subject to conditions available to all staff. Furthermore, the conflicts of interest framework and decision-making process may differentiate between material and non-material loans or other material transactions, different types of loans and other transactions and the level of actual or potential conflicts of interest they may create.

114. As part of the conflicts of interest framework, the management body should set appropriate thresholds (e.g. per product type, volume, or depending on the conditions) above which the transaction with a member of the management body or its related parties always requires approval by the management body. Decisions on material loans and other material transactions with members of the management body that are not being concluded under normal market terms, but subject to conditions available to all staff, should always be made by the management body.

115. The member of the management body benefiting from such a material loan or other material transaction, or the member who is related to the counterparty, should not be involved in the decision-making process.

116. When deciding on a loan or other transaction with a member of the management body or their related parties, before taking a decision investment firms should assess the risk to which the investment firm might be exposed due to the transaction.

117. To ensure compliance with their conflicts of interest policies, investment firms should ensure that all relevant internal control procedures fully apply to loans and other transactions with members of the management body or their related parties and that an appropriate oversight framework is in place at the level of the management body in its supervisory function.

11.2 Documentation of loans to members of the management body and their related parties and additional information

[31] Business transactions include loan leasing, factoring, services in the context of initial public offerings (IPOs), mergers and acquisitions and buying and selling property.

118. For the purposes of Article 26 of Directive (EU) 2019/2034, investment firms should document data on loans to members of the management body and their related parties properly, including at least:

a. the name of the debtor and their status (i.e. member of the management body or related party) and, with regard to loans to a related party, the member of the management body to whom the party is related and the nature of the relationship to the related party;

b. the type/nature of loan and the amount;

c. the terms and conditions applicable to the loan;

d. the date of approval of the loan;

e. the name of the individual or body and its composition taking the decision to approve the loan and the applicable conditions;

f. the fact (yes/no) as to whether or not the loan has been granted at market conditions; and

g. the fact (yes/no) as to whether or not the loan has been granted at conditions available to all staff.

119. Investment firms should ensure that the documentation of all loans to members of the management body and their related parties is complete and updated and that the investment firm is able to make available to competent authorities the complete documentation in an appropriate format upon request and without undue delay.

12 Internal alert procedures

120. Investment firms should put in place and maintain appropriate internal alert policies and procedures for staff to report potential or actual breaches of Regulation (EU) No 2033/2019 and national provisions transposing Directive (EU) 2019/2034 through a specific, independent and autonomous channel. It should not be necessary for reporting staff to have evidence of a breach; however, they should have a sufficient level of certainty that provides sufficient reason to launch an investigation. Investment firms should also implement appropriate processes and procedures that ensure that they comply with their obligations under the national implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

121. To avoid conflicts of interest, it should be possible for staff to report breaches outside regular reporting lines (e.g. through the compliance function, the internal audit function or an independent internal whistleblowing procedure). The alert procedures should ensure the

protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679[32] (GDPR).

122. The alert procedures should be made available to all staff within an investment firm.

123. Information provided by staff through the alert procedures should, if appropriate, be made available to the management body and other responsible functions defined within the internal alert policy. Where required by the staff member reporting a breach, the information should be provided to the management body and other responsible functions in an anonymised way. Investment firms may also provide for a whistleblowing process that allows information to be submitted in an anonymised way.

124. Investment firms should ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment. The investment firm should ensure that no person under the investment firm's control engages in the victimisation of a person who has reported a breach and should take appropriate measures against those responsible for any such victimisation.

125. Investment firms should also protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person. If measures are taken, the investment firms should take them in a way that aims to protect the person concerned from unintended negative effects that go beyond the objective of the measure taken.

126. In particular, internal alert procedures should:

    a. be documented (e.g. staff handbooks);

    b. provide clear rules that ensure that information on the reporting and the reported persons and the breach are treated confidentially, in accordance with Regulation (EU) 2016/679, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings;

    c. protect staff who raise concerns from being victimised because they have disclosed reportable breaches;

    d. ensure that the potential or actual breaches raised are assessed and escalated, including as appropriate to the relevant competent authority or law enforcement agency;

[32] Regulation (EU) 2016/679 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)

e. ensure, where possible, that confirmation of receipt of information is provided to staff who have raised potential or actual breaches;

f. ensure the tracking of the outcome of an investigation into a reported breach; and

g. ensure appropriate record keeping.

13 Reporting of breaches to competent authorities

127. In accordance with article 22 of Directive (EU) 2019/2034, competent authorities should establish effective and reliable mechanisms to enable investment firms' staff to report to competent authorities relevant potential or actual breaches of Regulation (EU) No 2019/2033 and national provisions transposing Directive (EU) 2019/2034. These mechanisms should include, as a minimum:

a. specific procedures for the receipt of reports on breaches and follow-up, for instance a dedicated whistleblowing department, unit or function;

b. appropriate protection as referred to in Section 13;

c. protection of the personal data of both the natural person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679 (GDPR); and

d. clear procedures as set out in Section 12.

128. Without prejudice to the possibility of reporting breaches through the competent authorities' mechanisms, competent authorities may encourage staff to first try and seek to use their investment firms' internal alert procedures.

Title V – internal control framework and mechanisms

14 Internal control framework

129. Investment firms should develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the investment firms and a robust and comprehensive internal control framework. Under this framework, investment firms' business lines should be responsible for managing the risks they incur in conducting their activities and should have controls in place that aim to ensure compliance with internal and external requirements. As part of this framework, investment firms should have a permanent and effective internal compliance function[33] with appropriate and sufficient authority, stature and access to the management body to fulfil its mission, and a risk management framework.

[33] Without prejudice to Article 22 of the EU Commission Delegated Regulation 565/2017

Where proportionate taking into account the criteria listed in Title I, investment firms should also have an internal risk management and audit function.

130. The internal control framework of the investment firm concerned should be adapted on an individual basis to the specificity of its business, its complexity and the associated risks, taking into account the group context. The investment firm concerned should organise the exchange of the necessary information in a manner that ensures that each management body, business line and internal unit, including each internal control function, is able to carry out its duties. This means, for example, a necessary exchange of adequate information between the business lines and the compliance function, and the AML/CFT compliance function where it is a separate control function, at the group level and between the heads of the internal control functions at the group level and the management body of the investment firms.

131. Investment firms should implement appropriate processes and procedures to ensure that they comply with their obligations in the context of combating money laundering and terrorist financing. Investment firms should assess their exposure to the risk that they may be used for the purpose of ML/TF and, where necessary, take mitigating measures to reduce those risks as well as the operational and reputational risks linked to them. Investment firms should take measures to ensure that their staff are aware of such ML/TF risks and the impact that ML/TF has on the investment firm and the integrity of the financial system.

132. The internal control framework should cover the whole organisation, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.

133. The internal control framework of an investment firm should ensure:

    a. effective and efficient operations;

    b. adequate identification, measurement and mitigation of risks;

    c. the reliability of financial and non-financial information reported both internally and externally;

    d. sound administrative and accounting procedures; and

    e. compliance with laws, regulations, supervisory requirements and the investment firm's internal policies, processes, rules and decisions.

15 Implementing an internal control framework

134. The management body should be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for

overseeing all business lines and internal units, including internal control functions (such as compliance including AML/CFT compliance where separate from the compliance function, and risk management and internal audit functions where established). Investment firms should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which should be approved by the management body. Where no risk management function is established, the management body should be responsible for establishing and monitoring adequate risk management procedures and policies.

135. An investment firm should have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines, internal units and internal control functions.

136. Investment firms should communicate these policies, mechanisms and procedures to all staff and every time material changes have been made.

137. The internal control functions should verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.

138. Internal control functions should regularly submit to the management body written reports on major deficiencies that have been identified. These reports should include, for each new major deficiency identified, the relevant risks involved, an impact assessment, recommendations and corrective measures to be taken. The management body should follow up on the findings of the internal control functions in a timely and effective manner and require adequate remedial actions. A formal follow-up procedure on findings and corrective measures taken should be put in place.

16 Risk management framework

139. As part of the overall internal control framework, investment firms should have a holistic investment firm-wide risk management framework extending across all their business lines and internal units, including internal control functions, recognising fully the economic substance of all their risk exposures including the risks the investment firm poses to itself, its customers and markets and liquidity risks, in particular those that can have a material impact on or deplete the level of own funds available. The risk management framework should enable the investment firm to make fully informed decisions on risk-taking. The risk management framework should encompass all risks as well as actual risks and future risks that the investment firm may be exposed to. Risks should be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the investment firm and at a consolidated level. All relevant risks should be encompassed in the risk management framework with appropriate consideration given to both financial and non-financial risks, including market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance with AML/CTF and other financial crime, ESG and strategic risks.

140. An investment firm's risk management framework should include policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks at the business line, investment firm and consolidated levels.

141. An investment firm's risk management framework should provide specific guidance on the implementation of its strategies. This guidance should, where appropriate, establish and maintain internal limits consistent with the investment firm's risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. An investment firm's risk profile should be kept within these established limits. The risk management framework should ensure that, whenever breaches of risk limits occur, there is a defined process to escalate and address them with an appropriate follow-up procedure.

142. The risk management framework should be subject to independent internal review, e.g. performed by the internal audit function, and reassessed regularly against the investment firm's risk appetite, taking into account information from the risk management function and the risk committee, where established. Factors that should be considered include internal and external developments, including revenue changes; any increase in the complexity of the investment firm's business, risk profile or operating structure; geographic expansion; mergers and acquisitions; and the introduction of new products or business lines.

143. When identifying and measuring or assessing risks, an investment firm should develop appropriate methodologies including both forward-looking and backward-looking tools. The tools should include the assessment of the actual risk profile against the investment firm's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the investment firm's risk capacity. The tools should provide information on any adjustment to the risk profile that may be required. Investment firms should make appropriately conservative assumptions when building stressed scenarios.

144. Investment firms should take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models (e.g. the exclusion of some relevant risks) rather than a superior strategy or excellent execution of a strategy on the part of the investment firm. The determination of the level of risk taken should not therefore be based only on quantitative information or model outputs; it should also comprise a qualitative approach (including expert judgement and critical analysis). Relevant macroeconomic environmental trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios.

145. The ultimate responsibility for risk assessment lies solely with the investment firm, which, accordingly, should evaluate its risks critically and should not rely exclusively on external assessments.

146. Investment firms should be fully aware of the limitations of models and metrics and use not only quantitative but also qualitative risk assessment tools (including expert judgement and critical analysis).

147. In addition to the investment firms' own assessments, investment firms may use external risk assessments (including external credit ratings or externally purchased risk models). Investment firms should be fully aware of the exact scope of such assessments and their limitations.

148. Regular and transparent reporting mechanisms should be established so that the management body, its risk committee, where established, and all relevant units in an investment firm are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant information about the identification, measurement or assessment, monitoring and management of risks. The reporting framework should be well defined and documented.

149. Effective communication and awareness regarding risks and the risk strategy is crucial for the whole risk management process, including the review and decision-making processes, and helps prevent decisions that may unknowingly increase risk. Effective risk reporting involves sound internal consideration and the communication of the risk strategy and relevant risk data (e.g. exposures and key risk indicators), both horizontally across the investment firms and up and down the management chain.

17 Internal control functions

150. The internal control functions should include an effective and permanent internal compliance function, and where appropriate and proportionate, taking into account the criteria listed in Title I, a risk management function and an internal audit function. The responsibilities of control functions also include ensuring compliance with AML/CTF requirements. Where investment firms do not establish and maintain a risk management function and an internal audit function, they should be able to demonstrate upon request that the policies and procedures adopted and implemented for an internal control framework effectively achieve the same outcome as the guidelines provided in this Title V.

151. Where the investment firm does not establish an internal risk management function (RMF) or internal audit function (IAF), the responsibilities of these functions as set out in these guidelines are with the staff in charge of the established procedures and ultimately the management body, who may delegate the operational tasks internally or externally.

152. Without prejudice to national law implementing Directive (EU) 2015/849, institutions should assign the responsibility for ensuring the institution's compliance with the requirements of that directive and the institution's policies and procedures to a staff member (e.g. head of compliance). Institutions may establish a separate AML/CTF compliance function as an independent control function. The person responsible for AML/CTF should, where necessary, be able to report directly to the management body in its management and its supervisory function.

17.1 Heads of the internal control functions

153. Heads of internal control functions should be established at an adequate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil his or her responsibilities. The head of compliance and, where established, the heads of the risk management and internal audit functions should report and be directly accountable to the management body, and their performance should be reviewed by the management body.

154. Where necessary, the heads of internal control functions should be able to have access and report directly to the management body in its supervisory function to raise concerns and warn the supervisory function, where appropriate, when specific developments affect or may affect the investment firms. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well.

155. Investment firms should have documented processes in place to assign the position of the head of an internal control function and for withdrawing his or her responsibilities. In any case, the heads of internal control functions should not be removed without the prior approval of the management body in its supervisory function.

17.2 Independence of internal control functions

156. In order for the internal control functions to be regarded as operating independently, the following conditions should be met:

a. their staff do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control unless it is demonstrated that, in view of the criteria listed in Title I for the application of the proportionality principle, the internal control functions continue to be effective. In that case, investment firms should assess whether the effectiveness of their internal control functions is compromised.

b. Where appropriate, they are organisationally separate from the activities they are assigned to monitor and control;

c. the remuneration of the internal control functions staff should not be linked to the performance of the activities the internal control function monitors and controls, and should not otherwise be likely to compromise the staff members' objectivity[34].

17.3 Resources of internal control functions

[34] See also the EBA guidelines on sound remuneration policies, available at https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

157. Internal control functions should have sufficient resources. Taking into account the application of the proportionality principle as set out in Title I, they should have an adequate number of qualified staff (at both the parent and subsidiary levels). Staff should remain qualified on an ongoing basis and should receive training as necessary.

158. Internal control functions should have appropriate IT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities. They should have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the investment firm.

18 Risk management function

159. The risk management function (RMF) should cover the whole investment firm. The RMF should have sufficient authority, stature and resources, taking into account the proportionality criteria listed in Title I, to implement risk policies and the risk management framework as set out in Section 17.

160. The RMF should have, where necessary, direct access to the management body in its supervisory function and its committees, where established, including in particular the risk committee.

161. The RMF should have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.

162. Staff within the RMF should possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures, and markets and products, and should have access to regular training.

163. The RMF should be a central organisational feature of the investment firm, structured so that it can implement risk policies and control the risk management framework. The RMF should play a key role in ensuring that the investment firm has effective risk management processes in place. The RMF should be actively involved in all material risk management decisions.

164. In a group, the RMF in the Union parent undertaking should be able to deliver a group-wide holistic view on all risks and to ensure that the risk strategy is complied with.

165. The RMF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or internal units, and should inform the management body as to whether such information and advice is consistent with the investment firm's risk strategy and risk appetite. The RMF may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.

18.1 RMF's role in risk strategy and decisions

166. The RMF should be actively involved at an early stage in developing the investment firm's risk strategy and ensuring that the investment firm has effective risk management processes in place. The RMF should provide the management body with all relevant risk-related information to enable it to set the investment firm's risk appetite level. The RMF should assess the robustness and sustainability of the risk strategy and appetite. It should ensure that risk appetite is appropriately translated into specific risk limits. The RMF should also assess the risk strategies of business units, including targets proposed by the business units, and should be involved before a decision is made by the management body concerning the risk strategies and risk appetite. Targets should be plausible and consistent with the investment firm's risk strategy and risk appetite.

167. The RMF's involvement in decision-making processes should ensure that risk considerations are taken into account appropriately. However, accountability for the decisions taken should remain with the business and internal units, and ultimately the management body.

18.2 RMF's role in material changes

168. Before decisions on material changes to processes or systems or exceptional transactions are taken, the RMF should be involved in the evaluation of the impact of such changes and exceptional transactions on the investment firm's and group's overall risk, and should report its findings directly to the management body before a decision is taken.

169. The RMF should evaluate how the risks identified could affect the investment firm's or group's ability to manage its risk profile, liquidity and its sound capital base under normal and adverse circumstances.

18.3 RMF's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting on risks

170. The RMF should ensure that that there is an appropriate risk management framework and that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the investment firm.

171. The RMF should ensure that identification and assessment are not based only on quantitative information or model outputs, but also take into account qualitative approaches. The RMF should keep the management body informed of the assumptions used in, and the potential shortcomings of, the risk models and analysis.

172. The RMF should ensure that transactions with related parties are reviewed and that the risks they pose for the investment firm are identified and adequately assessed.

173. The RMF should ensure that all identified risks are effectively monitored by the business units.

174. The RMF should regularly monitor the actual risk profile of the investment firm and scrutinise it against the investment firm's strategic goals and risk appetite to enable decision-making by the management body in its management function and challenges by the management body in its supervisory function.

175. The RMF should analyse trends and recognise new or emerging risks and increases in risk arising from changing circumstances and conditions. It should also regularly review actual risk outcomes against previous estimates (i.e. back testing) to assess and improve the accuracy and effectiveness of the risk management process.

176. The RMF should evaluate possible ways to mitigate risks. Reporting to the management body should include proposals for appropriate risk-mitigating actions.

18.4 RMF's role in limits

177. The RMF should independently assess breaches of risk appetite or limits (including ascertaining the cause and undertaking a legal and economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it). The RMF should inform the business units concerned and the management body, and recommend possible remedies. The RMF should report directly to the management body in its supervisory function when the breach is material, without prejudice for the RMF to report to other internal functions and committees.

178. The RMF should play a key role in ensuring that a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the management body and, where established, the risk committee.

18.5 Head of the risk management function

179. Where established, the head of the RMF should be responsible for providing comprehensive and understandable information on risks and advising the management body, enabling this body to understand the investment firm's overall risk profile. The same applies to the head of the RMF of a parent investment firm regarding the consolidated situation. Where no independent function has been established, the responsibilities of the head of the risk management function lie with the staff to whom the risk management procedures are entrusted or the members of the management body directly.

180. The head of the RMF should have sufficient expertise, independence and seniority to challenge decisions that affect an investment firm's exposure to risks. Where the head of the RMF is not a member of the management body, taking into account the principle of proportionality as set out in Title I, investment firms should appoint an independent head of the RMF who has no responsibilities for other functions and reports directly to the management body. Where it is not proportionate to appoint a person who is dedicated only to the role of head of the RMF, taking into account the principle of proportionality as set out in Title I, this function can be

combined with the head of the compliance function or can be performed by another senior person, provided there is no conflict of interest between the tasks performed. In any case, this person should have sufficient authority, stature and independence (e.g. head of legal).

181. The head of the RMF should be able to challenge decisions taken by the investment firm's management and its management body, and the grounds for objections should be formally documented. If an investment firm wishes to grant the head of the RMF the right to veto decisions (e.g. a credit or investment decision or the setting of a limit) made at levels below the management body, it should specify the scope of such a veto right, the escalation or appeal procedures, and how the management body will be involved.

182. Investment firms should establish strengthened processes for the approval of decisions on which the head of the RMF has expressed a negative view. In its supervisory function, the management body should be able to communicate directly with the head of the RMF on key risk issues, including developments that may be inconsistent with the investment firm's risk strategy and risk appetite.

19 Compliance function[35]

183. Investment firms should establish a permanent and effective compliance function to manage compliance risk, and should appoint a person to be responsible for this function across the entire investment firm (the compliance officer). The compliance function, policies and procedures should also be compliant with Article 22 of Commission Delegated Regulation (EU) 2017/565 and ESMA guidelines on the compliance function.

184. The role of compliance officer, taking into account the principle of proportionality as set out in Title I, can be combined with the head of the RMF or, where it is not proportionate to appoint a person who is dedicated only to this function, can be performed by another senior person (e.g. head of legal), provided there is no conflict of interest between the tasks performed.

185. Staff within the compliance function should possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and should have access to regular training.

186. The management body in its supervisory function should oversee the implementation of a well-documented compliance policy, which should be communicated to all staff. Investment firms should set up a process to regularly assess changes in the law and regulations applicable to its activities.

187. The compliance function should advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess

[35] This section should be read without prejudice and in conjunction with the ESMA guidelines on the compliance function.

the possible impact of any changes in the legal or regulatory environment on the investment firm's activities and compliance framework.

188. The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed. The compliance function should report to the management body and communicate as appropriate with the RMF on the investment firm's compliance risk and its management. The compliance function and the RMF should cooperate and exchange information as appropriate to perform their respective tasks. The findings of the compliance function should be taken into account by the management body and the RMF in decision-making processes.

189. Investment firms should take appropriate action against internal or external behaviour that could facilitate or enable fraud, ML/TF or other financial crime and breaches of discipline (e.g. breaches of internal procedures or breaches of limits).

190. Investment firms should ensure that their subsidiaries and branches take steps to ensure that their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the compliance officer or the head of compliance of the Union parent undertaking.

20 Internal audit function

191. Where established, the IAF should be independent and have sufficient authority, stature and resources. In particular, investment firms should ensure that the qualification of the IAF's staff members and the IAF's resources, in particular its auditing tools and risk analysis methods, are adequate for the investment firm's size and locations, and the nature, scale and complexity of the risks associated with the investment firm's business model, activities, risk culture and risk appetite.

192. The IAF should be independent of the audited activities. Therefore, the IAF should not be combined with other functions.

193. The IAF should, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of an investment firm, including outsourced activities, with the investment firm's policies and procedures and with external regulatory requirements. Each entity within the group should fall within the scope of the IAF.

194. The IAF should not be involved in designing, selecting, establishing or implementing specific internal control policies, mechanisms, procedures or risk limits. However, this should not prevent the management body in its management function from requesting input from internal audit on matters relating to risk, internal controls and compliance with applicable rules.

195. The IAF should assess whether the investment firm's internal control framework as set out in Section 15 is both effective and efficient. In particular, the IAF should assess:

    a. the appropriateness of the investment firm's governance framework;

    b. whether existing policies and procedures remain adequate and comply with legal and regulatory requirements and with the risk strategy and risk appetite of the investment firm;

    c. the compliance of the procedures with the applicable laws and regulations and with decisions of the management body;

    d. whether the procedures are correctly and effectively implemented (e.g. compliance of transactions, the level of risk effectively incurred, etc.); and

    e. the adequacy, quality and effectiveness of the controls carried out and the reporting conducted by the business units (first line of defence) and the risk management and compliance functions.

196. The IAF should verify, in particular, the integrity of the processes ensuring the reliability of the investment firm's methods and techniques, and the assumptions and sources of information used in its internal models (e.g. risk modelling and accounting measurements). It should also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken.

197. The IAF should have unfettered investment firm-wide access to all the records, documents, information and buildings of the investment firms. This should include access to management information systems and minutes of all committees and decision-making bodies.

198. The IAF should adhere to national and international professional standards. An example of the professional standards referred to here is the standards established by the Institute of Internal Auditors.

199. Internal audit work should be performed in accordance with an audit plan and a detailed audit programme following a risk-based approach.

200. An internal audit plan should be drawn up at least once a year on the basis of the annual internal audit control objectives. The internal audit plan should be approved by the management body.

201. All audit recommendations should be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely resolution.

Title VI – business continuity management

202. Investment firms should establish a sound business continuity management and recovery plan to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption.

203. Investment firms may establish a specific independent business continuity function.

204. An investment firm's business relies on several critical resources (e.g. IT systems, including cloud services, communication systems, core staff and buildings). The purpose of business continuity management is to reduce the operational, financial, legal, reputational and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the investment firm's ordinary business procedures. Other risk management measures might be intended to reduce the probability of such incidents or to transfer their financial impact to third parties (e.g. through insurance).

205. In order to establish a sound business continuity management plan, an investment firm should carefully analyse risk factors for, and its exposure to, severe business disruptions and assess (quantitatively and qualitatively) their potential impact, using internal and/or external data and scenario analysis. This analysis should cover all business lines and internal units, including the RMF or risk management procedures, and should take into account their interdependency. The results of the analysis should contribute to defining the investment firm's recovery priorities and objectives.

206. On the basis of the abovementioned analysis, an investment firm should put in place:

    a. contingency and business continuity plans to ensure that the investment firm reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures; and

    b. recovery plans for critical resources to enable the investment firm to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions should be consistent with the investment firm's risk appetite.

207. Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business lines, internal units and RMF for staff in charge of risk management procedures, and should be stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training should be provided. Plans should be regularly tested and updated. Any challenges or failures occurring in the tests should be documented and analysed, with the plans reviewed accordingly.

Title VII – transparency

208. Strategies, policies and procedures should be communicated to all relevant staff throughout an investment firm. An investment firm's staff should understand and adhere to policies and procedures pertaining to their duties and responsibilities.

209. Accordingly, the management body should inform and update the relevant staff about the investment firm's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means.

210. Where parent undertakings are required by competent authorities under Article 44 of Directive (EU) 2019/2034 to publish annually a description of their legal structure and governance and the organisational structure of the group of investment firms, the information should include all entities within the group structure as defined in Directive (EU) 2013/34[36], by country.

211. The publication should include at least:

    a. an overview of the internal organisation of the investment firm and the group structure as defined in Directive (EU) 2013/34 and changes thereto, including the main reporting lines and responsibilities;

    b. any material changes since the previous publication and the date of the material change;

    c. new legal, governance or organisational structures;

    d. information on the structure, organisation and members of the management body, including the number of its members and the number of those qualified as independent, and specifying the gender and duration of the mandate of each member of the management body;

    e. the key responsibilities of the management body;

    f. a list of the committees of the management body in its supervisory function and their composition;

    g. an overview of the conflicts of interest policy applicable to the investment firm and to the management body;

    h. an overview of the internal control framework; and

[36] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19)

i. an overview of the business continuity management framework.

Annex I – aspects to take into account when developing an internal governance policy

In line with Title III, investment firms should consider the following aspects when documenting internal governance policies and arrangements:

1. Shareholder structure
2. Group structure, if applicable (legal and functional structure)
3. Composition and functioning of the management body
    a) selection criteria including how diversity is taken into account
    b) number, length of mandate, rotation, age
    c) independent members of the management body
    d) executive members of the management body
    e) non-executive members of the management body
    f) internal division of tasks, if applicable
4. Governance structure and organisation chart (with impact on the group, if applicable)
    a) specialised committees
        i. composition
        ii. functioning
    b) executive committee, if any
        i. composition
        ii. functioning
5. Key function holders
    a) head of the risk management function
    b) head of the compliance function
    c) head of the internal audit function
    d) chief financial officer
    e) other key function holders
6. Internal control framework
    a) description of each function, including its organisation, resources, stature and authority
7. Description of the risk strategy and risk management framework

8. Organisational structure (with impact on the group, if applicable)
    a) operational structure, business lines, and allocation of competences and responsibilities
    b) outsourcing
    c) range of products and services
    d) geographical scope of business
    e) provision of services under the regime of freedom of provision of services
    f) branches
    g) subsidiaries, joint ventures, etc.
    h) use of offshore centres
9. Code of conduct and behaviour (with impact on the group, if applicable)
    a) strategic objectives and company values
    b) internal codes and regulations, including anti money laundering and counter terrorism financing policies
    c) conflict of interest policy
    d) whistleblowing
10. Status of the internal governance policy, with date
    a) development
    b) last amendment
    c) last assessment
    d) approval by the management body.

5. Accompanying documents

5.1. Cost-benefit analysis/impact assessment

1. Article 16(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) (EBA Regulation) provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

   A. Problem identification and policy objectives

2. Directive (EU) 2019/2034 is setting out specific requirements on internal governance arrangements for investment firms that are not small and not interconnected. The EBA has been mandated under Article 26 Directive (EU) 2019/2034 to issue guidelines, in consultation with ESMA, on the application of the governance arrangements referred to in paragraph 1 of this Article.

   B. Baseline scenario

3. The current EU legislative framework for investment firms' governance arrangements mainly consists of Directive 2013/36/EU, Directive 2014/65/EU, the Commission Delegated Regulation (EU) 2017/565 and the Commission Delegated Directive (EU) No 2017/593, the EBA guidelines on sound remuneration policies, the joint EBA and ESMA guidelines on the assessment of the suitability of members of the management body and key function holders, the ESMA guidelines on certain aspects of the MiFID II compliance function requirements, the ESMA guidelines on product governance and the ITS guidelines on disclosures.

4. The impact assessment covers guidelines developed to ensure the harmonised application of investment firms' governance requirements introduced by Directive (EU) 2019/2034 where they differ from the previously applicable framework and from the MiFID framework. Areas that have not changed in substance and the changes introduced within the Directive (EU) 2019/2034 (IFD) and Regulation (EU) 2019/2033 have not been assessed.

   C. Options considered

   Implementation date

5. Specific governance requirements are being introduced for investment firms by implementing Directive (EU) 2019/2034 into national law on 26 June 2021.

6. Considering that the IFD governance framework as such is equivalent to the requirements under the CRD, a short implementation period is sufficient. However, some of the requirements under the IFD require some limited changes to investment firms' internal governance arrangements and documentation. This concerns e.g. the establishment of a risk committee and a remuneration committee for investment firms whose value of on and off-balance sheet assets is on average more than EUR 100 million over the four-year period immediately preceding the given financial year, but also the diversity aspect and the conflicts of interest policy regarding related-party transactions. A few investment firms have previously not been subject to the CRD requirements. Hence, an application date of the guidelines that specify these requirements in detail of 30 April 2022 appears appropriate.

Risk committee

7. The IFD requires investment firms that have on and off-balance sheet assets of on average more than EUR 100 million over the four-year period immediately preceding the given financial year to establish a risk committee. Guidance has been provided on the composition and tasks of this committee.

8. Option A: the guidelines should follow exactly the same approach regarding the composition of this committee as for CRD institutions to ensure a consistent approach among sectors.

9. Option B: the guidelines should follow a more proportionate approach, taking into account the nature and complexities of investment firms' activities. Where the number of members within the management body in its supervisory function is insufficient to ensure a sound composition of committees as set out in this section, the tasks of the committee may be delegated to one member of the management body in its supervisory function, who is supported as appropriate by staff. Committees may be composed of the same group of members, taking into account the criteria set out in Title I and the number of independent members of the management body in its supervisory function and the specific experience, knowledge and skills that are individually or collectively required for the committees. The reasoning for the composition of committees should be documented.

   Option A would lead to some additional costs for investment firms compared to Option B. Option B follows a more proportionate approach to setting up committees.

   Option B has been retained.

Loans and other transactions with members of the management body and their related parties

10. Related party transactions are a specific source of actual or potential conflicts of interest, and specific guidance has been developed for the prudent management of conflicts of

interest that might be created by such transactions and to ensure that firms have appropriate decision management and oversight processes for such transactions.

11. Option A: replicate the same approach taken under the CRD, adapting it to investment firms' business models and with a more proportionate approach taken into account. Indeed, investment firms do not usually grant loans other than in specific cases.

12. Option B: not providing guidelines on related party transactions

    Regarding option A, the objective of the changes is to ensure that there is sufficient scrutiny in respect of decisions regarding such loans when they are granted and other transactions and that conflicts of interest in this context are managed appropriately. Not providing guidance on this aspect would not be effective and would not ensure that investment firms have sound governance arrangements in line with the IFD and MiFID. Documentation of loans is required to monitor the relevant practices.. In this case, investment firms should document loans with their management body and their related party. Minor additional costs are created, caused by specific additional documentation requirements that are necessary to ensure that the impact of such loans and the conflicts of interest they potentially create can be assessed by firms and competent authorities. However the level of detail has been reduced to take into account the fact that investment firms do not usually grant loans. In line with the principle of proportionality, the guidelines differentiate between requirements for material and non-material loans.

Option A was retained

Diversity and gender-neutral pay

13. The guidelines aim to further specify requirements under the IFD and to achieve harmonisation at the EU level. Given the need for Member States to implement the IFD provisions and to abide by the principles set out within the European Charter of Fundamental Rights, it is presumed that the guidelines do not lead to any conflicts regarding these matters. Investment firms' policies must be gender-neutral. Some aspects concerning equal opportunities and anti-discrimination have been further specified in the guidelines. In the same way as for CRD institutions, investment firms are required to document and monitor the trend in the gender pay gap.

14. Option A: replicate the same approach taken under the CRD.

15. Option B: adapting it to investment firms' business models and with a more proportionate approach. Indeed, monitoring the trend in the gender pay gap could be required only where investment firms have 50 or more staff in accordance with the threshold foreseen under the Commission recommendation of 7 March 2014 on strengthening the principle of equal pay between men and women through transparency.

Option A would lead to some additional burdens for investment firms compared to option B.

Option B was retained.

Internal control framework and the three lines of defence.

16. Option A: requiring Class 2 firms to set up three independent functions (compliance, risk management and internal audit functions)

17. Option B: establishing a more proportionate approach, also to be consistent with the MiFID framework; a permanent and effective compliance function should be set up; firms are not required to set up an internal risk management function, where justified. However, firms should implement policies and process to achieve the same objectives and should have a sound and effective internal control framework.

18. Option A is not recommended, as it does not lead to greater sectoral consistencies. It would cause additional costs to establish a sound internal control framework and ensure the independence of the internal control functions.

19. Option B is recommended to create consistency between the MiFID and CRD frameworks. By implementing policies and processes to achieve the same objectives, firms would still benefit from an effective framework, which would lead to a better alignment of the risk profile with risk appetite as set by the management body.

    Option B was retained.

E. Cost-benefit analysis

20. Given the limited changes compared to the baseline scenario and the easing of some requirements within the IFD, and given that most of the governance arrangements already exist under the MiFID framework, it is assumed that the changes to the guidelines create low implementation costs, mainly for updates to internal policies and the additional documentation required.

5.2. Feedback on the public consultation and opinion of the Banking Stakeholder Group

Summary of key issues and the EBA's response

The EBA published its consultation paper on 17 December 2020 and received 10 responses in total. Eight of them were published, while one was submitted on a confidential basis. The Banking Stakeholder Group did not submit its views. The last response was submitted too late and will therefore not be published. The consultation concerned the whole draft guidelines on internal governance under the IFD, which complete the various governance provisions in Directive (EU) 2019/2034.

The main comments received challenged the fact that the draft guidelines are based on the current guidelines on internal governance, which – according to the respondents – is not in line with the intention of the IFD, which establishes a simplified and proportionate regime for investment firms. The respondents consider the draft guidelines to be too extensive for investment firms covered by them.

In addition, some respondents believed that the draft guidelines do not take into account the internal governance requirements set out under MiFID II and the Commission Delegated Regulation (EU) 2017/565, which in particular include specific provisions regarding internal control functions, whistleblowing schemes and conflicts of interest policies. They point out that dual regulation in this area is unjustified, unnecessary, and burdensome to investment firms.

A detailed analyses of the comments received is included in the feedback table below.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comments			
Guidelines on internal governance under the CRD	Several respondents comment that the draft GL are very similar to those currently in effect and applicable to CRD and MiFID firms. As the intention of the IFD is to put in place a prudential framework that is more appropriate for investment firms, the respondents urged the EBA to take a similar approach in considering the appropriate governance requirement for investment firms. The draft GL is too extensive for non-systemically important investment firms. They also feel that the GLs overlap with MiFID II and the Commission Delegated Regulation (EU) 2017/565 and suggest deleting all the requirements that are not covered by Article 26 IFD but are subject to MiFID II. One respondent is concerned that the concept of significant firms used in the CRR has been incorporated into the GL in relation to firms	Guidelines are in line with the mandate provided under Article 26 of the IFD and are consistent with the MiFID framework, including with Commission Delegated Regulation (EU) 2017/565. A careful assessment was made in cooperation with the ESMA. In accordance with the proportionality principle, the guidelines take into account the specificities of investment firms. Significant investment firms (class 1) are subject to the CRD/CRR framework. Investment firms for which the value of their on and off-balance sheet assets is on average more than EUR 100 million over the four-year period immediately preceding the given financial year must establish risk and remuneration committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this	No change

	with a balance sheet above EUR 100m. It is disproportionate to carry over the provisions – this applies only to significant CRR firms – to all IFD firms with a balance sheet above EUR 100m.	body. This is fully in line with Article 28 of the IFD. Another threshold can be specified by national law. Finally, it should be stressed that the guidelines on internal governance under the IFD do not apply to small and non-interconnected investment firms (class 3 firms).	
Scope of the guidelines on internal governance under the CRD	One respondent disagrees with the EBA's assessment that the CRD governance requirements already apply to all investment firms covered by the IFD governance rules. The definition of investment firms in the CRD/CRR does not encompass entities providing certain MiFID services without a licence to hold client money or to deal on their own account. For such limited licence firms that do not meet the thresholds in Article 12 IFR, the IFD framework lays down new governance requirements in addition to the MiFID.	Under CRD IV, a set of investments were already subject to governance requirements and were therefore included in this framework. Under CRD V, only class 2 firms are subject to governance requirements. It should be stressed, however, that all investment firms are subject to governance requirements under MIFID.	No change
Para. 24 Background	One respondent suggests clarifying that small and non-interconnected investment firms are not required to set up governance rules regarding liquidity risks on an intra-day basis as a standard process.	In accordance with Article 29 (3), competent authorities should ensure that small and non-interconnected investment firms have robust strategies, policies, processes and systems for the identification, measurement, management and monitoring of liquidity risk over an	No change

		appropriate set of time horizons, including intra-day, so as to ensure that the investment firm maintains adequate levels of liquid resources.	
Responses to questions in Consultation Paper EBA/CP/2020/27			
Q1. Are the subject matter, scope of application, definitions and date of application appropriate and sufficiently clear?			
Para. 1 Status of these guidelines	One respondent suggests replacing the term 'financial institutions, including investment firms' with the term 'investment firms covered by Article 26 of the Directive (EU) 2019/2034'.	The use of this wording is in line with the EBA's foundation as referred to in Article 4 (1) of Regulation (EU) No 1093/2010 and explicitly refers to investment firms as defined in Article 4(1)(1) of Directive 2014/65/EU.	No change
Para. 5 Subject matter	One respondent suggests clarifying the subject matter so that *'Section 2 of Chapter 2'* is amended to *'Article 26'*.	Section 2 of Chapter 2 refers to internal governance, transparency, treatment of risks and remuneration, so it is sufficiently clear. Article 26 refers only to a single provision.	No change
Para. 7 Addressees	One respondent suggests amending the addressees of the guidelines so that the scope of the guidelines is clearly limited to investment firms within the meaning of Article 2 IFD that are authorised and supervised under MiFID II, instead of financial institutions as referred to in	In accordance with Article 2 the IFD applies to investment firms authorised and supervised under Directive 2014/65/EU. In addition, the guidelines specify further that the governance requirements do not apply to small and non-interconnected investment firms (class 3 firms)	No change

	Article 4 (1) of Regulation (EU) No 1093/2010, which are investment firms as defined in Article 4(1)(1) of MiFID II.	as referred to under Article 12(1) of Regulation (EU) 2019/2033.	
Para. 8-14 Scope of application	One respondent suggests clarifying that the governance rules also cover the activities of investment firms providing portfolio management without a licence for dealing on their own account or holding client assets or money in an appropriate and proportionate way. The draft guidelines (in particular the requirements on the tasks and responsibilities of the risk management function) are only focused on the investment firms' risk profile.	In accordance with the IFD, the guidelines on internal governance apply to all investment firms that do not qualify as small and non-interconnected investment firms (class 3 firms) as referred to under Article 12(1) of Regulation (EU) 2019/2033. They also apply in a proportionate manner, and a section further specifies how to take into account the application of the proportionality principle.	No change
Para. 16 Date of application	Several respondents suggest postponing the date of application by at least 6 months.	The comment has been taken into account. The guidelines will enter into force on 30 April 2022. However, this does not change the fact that investment firms have to comply with the national implementation of the IFD when it comes into force.	Guidelines amended
Q2. Is Title II+(I) sufficiently clear? Do you think other criteria should be added or deleted as inappropriate?			
Title I – proportionality			

Para. 20 Proportionality	Several respondents comment that the description of proportionality is too complex and extensive since the criteria are difficult to assess in practice. This results in different assessments, which causes competitive disadvantages for some companies. In addition, a few respondents request clarification that in assessing what is proportionate, the focus should be on the combination of all the criteria mentioned since the amount of assets under management are not suitable or eligible to be a standalone criterion in order to ensure an appropriate implementation of the governance requirements. Some respondents suggest that institutions could be given the discretion to define the specific arrangements for the individual requirements – depending on the risk and complexity of their business model and risk profile.	The governance arrangements should be appropriate and proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the investment firm. This section further specifies how to take into account criteria for the application of the proportionality principle. This is not an exhaustive list, and an investment firm may also consider a combination of these criteria. When applying these criteria, investment firms should also be able to demonstrate to their CA that they are relevant to their businesses. The criteria listed further specify the principle of proportionality, are non-exhaustive and fully relevant to investment firms.	No change
Title II – role and composition of the management body			
Management body	One respondent suggests that the competences of the management body should be aligned with MiFID II.	The competence of the management body is consistent with the MiFID framework and in line with the IFD mandate under article 26.	No change

Para. 22-31 Role and responsibilities of the management body	One respondent suggests that employee/trade union representation is given a place on the management body in countries and companies where such representation is present.	The management body includes representatives of employees where applicable. There is no need to specify this point. This section is about the management body as a collegiate body.	No change
Para. 26 Role and responsibilities of the management body	One respondent requests clarifying that a 'suitable business model' does not mean an ESG business model with the requirement to ensure strategies are based on sustainable finance models.	The paragraph has been clarified.	Guidelines amended
Section 3 Supervisory function of the management body	One respondent suggests clarifying how investment firms should consider the application of these requirements, in particular para. 37 and 38 where the EBA suggests that national law would take precedence over EBA guidelines. One respondent asks for further clarification about the reference to section 9.3 of the joint ESMA and EBA guidelines on suitability as a reference to the independence criteria in paragraph 91 or to the categories of firms that are required to have independent directors in	The guidelines specify that the terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law. When implementing these guidelines, competent authorities should take into	No change

	paragraph 89. If the former, paragraph 37 exceeds the requirements of the level 1 text. If the latter, the guidelines should make it clear the reference made to the scope of application of the requirement to have independent directors and that the references therein to CRD firms do not provide sufficient clarity once investment firms become subject to the IFD. This is not supported by the level 1 text in terms of requirements to have independent directors.	account their national company law and specify, where necessary, to which body or members of the management body these functions should apply. Please refer to the EBA and ESMA guidelines on suitability. Under the updated joint EBA and ESMA guidelines on suitability, investment firms as defined in Article 4(1)(1) of Directive 2014/65/EU that do not meet all of the conditions for qualifying as small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033 and that are neither significant nor listed should, as a general principle, have at least one independent member on the management body in its supervisory function. However, competent authorities may not require any independent directors under specific conditions foreseen in the guidelines.	
Section 5 Committees of the management body	One respondent notes that the requirement to have separate governance committees conflicts with the proportionality objective of the IFD and asks that the guidelines are amended to enable firms that are treated as significant	In accordance with Article 28 of the IFD and unless otherwise specified by national law[37], investment firms for which the value of on and off-balance sheet assets is on average more than EUR 100 million over the four-year period	No change

[37] Article 28 of Directive (EU) 2019/2034 requires that Investment firms that do not meet the criteria set out in point (a) of Article 32(4) to establish a risk committee composed of members of the management body who do not perform any executive function in the investment firm concerned.

in its supervisory function	under IFD/IFR to implement proportionate structures.	immediately preceding the given financial year must establish risk and remuneration [38] committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body.	
Para. 49, 51 and 53 Composition of committees	One respondent suggests revising the provisions, which are not supported by the IFD, which includes no requirements for independent directors. This requirement is disproportionate in the light of CRD V requirements, which would have exempted non-significant CRD investment firms from the requirement generally.	The EBA must issue specific guidelines whenever explicitly required under European Union law. This is the case for Article 26, which mandates the EBA and ESMA to issue guidelines on governance arrangements, processes and internal control mechanisms. In addition, Article 16 of EBA Regulation (EU) No 1093/2010 lays down the general competence to issue guidelines ensuring the common, uniform and consistent application of Union within its scope of action law and effective supervisory practices within the ESFS. The same holds true for the ESMA. Accordingly, the guidelines do not go beyond the scope of their mandate. Independence is part of sound governance arrangements.	No change
Q3. Is Title III sufficiently clear and appropriate?			

[38] With regard to the remuneration committee, please refer to the EBA guidelines on sound remuneration practices under Directive (EU) 2019/2034.

Definitions of parent investment firms and their subsidiaries	One respondent requests reviewing all references to 'parent investment firms and their subsidiaries' and all other terms and definitions used in the group context. The terms used do not comply with the definitions and scope of the prudential consolidation of the IFD/IFR framework in all cases. Not every parent company of an investment firm group is an investment firm. This applies, in particular, to the general group approach in paragraph 77. The respondent disagrees with the scope definition stating that the 'parent investment firms and their subsidiaries' should ensure that governance arrangements are consistent and well-integrated on a consolidated basis.	The guidelines have been clarified and consistent terminology has been used for 'EU parent undertakings'. The group application section is fully in line with the IFD, which refers to the CRD/CRR framework in respect of this matter. Within a group context, the EU parent undertakings should ensure that governance arrangements are coherent and consistent within the group.	No change
Para. 83 Organisational framework in a group context	One respondent suggests clarifying how 'these guidelines apply irrespective of the fact that they may be subsidiaries of a parent investment firm in a third country'. The statement seems to be in conflict with the sentiment conveyed in para. 37 and 38 of the GL.	The guidelines apply to investment firms located in the EU irrespective of the fact that they may be subsidiaries of a parent investment firm in a third country. The guidelines have been clarified.	Guidelines amended
Q4. It Title IV appropriate and sufficiently clear? In particular the item on conflicts of interest and RPT at investment firms. Should we keep it like this?			

Para. 92 Corporate values and code of conduct	One respondent proposes adding that the proportionality principle should be considered when it comes to gender equality in management positions.	The guidelines have been clarified. Investment firms' policies should be gender-neutral.	Guidelines amended
Para. 10 Conflicts of interest policy at firm level	One respondent suggests clarifying whether investment firms are expected to establish a conflicts of interest policy in addition to the one that already exists within investment firms in order to comply with MiFID II and regulation 2017/565. Several respondents suggest deleting this part.	A separate policy is not required. However, the conflicts of interest policy should be in line and consistent with the framework under MiFID II and the Commission Delegated Regulation (EU) 2017/565 and also the IFD, as further specified in these guidelines.	No change
Para. 123 Internal alert procedures	One respondent suggests strengthening this paragraph by adding that the whistleblower's identity should be kept confidential and preferably anonymous for as long as possible.	In accordance with the IFD, the guidelines specify that where required by the staff member reporting a breach, the information should be provided to the management body and other responsible functions in an anonymised way. Investment firms may also establish a whistleblowing process that allows information to be submitted in an anonymised way.	No change
Para. 126(d)	One respondent would like clarification regarding this reference.	The guidelines have been clarified.	Guidelines amended

Reporting breaches to competent authorities			
Q5. Is Title V appropriate and sufficiently clear?			
Section 18-21 Internal control functions	A few respondents suggest excluding section 18-21 from the guidelines since MiFID II and Regulation (EU) 2017/565 include appropriate provisions on this matter. In addition, the ESMA has developed guidelines regarding the compliance function.	Consistency has been ensured with ESMA products.	No change
Para. 193 Internal audit function	One respondent would like clarification with regard to this reference.	The guidelines have been clarified.	Guidelines clarified
Q6. Is Title VI appropriate and sufficiently clear?			
Para. 200-205	One respondent suggests reviewing the provisions relating to the internal risk management requirements of supervised entities regarding ICT risks and activities since	The EBA will issue further guidance in line with the mandates received in the upcoming Directive.	No change

	this will be specified in the new Regulation (DORA).		
Business continuity management	One respondent suggests clarifying what is meant by 'appropriate' in terms of how often this training is provided and under what framework.	The appropriate frequency depends on the criticality of the process or system and staff awareness of such procedures.	No change