FMA

Document Number: 07 / 2018
Publication Date: 11.09.2018

FMA CIRCULAR

REGARDING THE ORGANISATIONAL REQUIREMENTS OF THE SECURITIES SUPERVISION ACT 2018 AND DELEGATED REGULATION (EU) 2017/565

("WAG 2018 ORGANISATIONAL CIRCULAR")

September 2018

TABLE OF CONTENTS

1. INTRODUCTION

1. The Austrian Financial Market Authority (FMA) refers in conjunction with the Securities Supervision Act 2018 (WAG 2018; Wertpapieraufsichtsgesetz 2018) and Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (hereafter the "Delegated Regulation") to the requirements regarding the functions of compliance pursuant to Article 22 of the Delegated Regulation,[1] complaints handling pursuant to Article 26 of the Delegated Regulation, risk management pursuant to Article 23 of the Delegated Regulation and internal audit pursuant to Article 24 of the Delegated Regulation and Article 32 WAG 2018 (risk management and internal audit).

2. The present circular was originally published in 2009, was revised in 2015 and is republished in this current updated version to take into consideration the WAG 2018 in conjunction with the Delegated Regulation. The most recently published version is valid.

3. This circular is aimed at legal entities as defined in Article 26 para. 1 WAG 2018, and is therefore addressed to the following entities:

   - **Credit institutions**, which provide investment services and activities on the basis of a licence pursuant to Article 1 para. 1 and para. 3 BWG;

   - **Insurance undertakings**, which pursuant to Article 6 para. 3 VAG 2016 broker shares/units of investment funds, and for which with regard to such activities, the exhaustive list of provisions of the WAG 2018 listed in Article 2 para. 2 WAG 2018 apply;

   - **Management companies** pursuant to Article 5 para. 1 InvFG 2011 that in addition also perform portfolio management and investment advice for individuals pursuant to

[1] The compliance function, the risk management function, and the internal audit function are also stipulated as being the key functions in the Solvency II Directive as well as in the joint EBA/ESMA Guidelines on the assessment of the suitability of members of the management body and key function holders (hereafter EBA/GL/2017/12). With regard to the latter publication, see also FMA Circular on Fit and Proper testing of directors, members of the supervisory board and key function folders (Hereafter "FMA Fit & Proper Circular") published in August 2018 (FMA Circular 06/2018). EBA Guidelines EBA/GL/2017/12 replace the existing EBA Guidelines published on 22.11.2012 (EBA/GL/2012/06) and are applicable with effect from 30.06.2018.

Article 5 para. 2 nos. 3 and 4 InvFG 2011, as well as **AIFMs** (Alternative Investment Fund Managers) pursuant to Article 4 AIFMG, who additionally offer individual portfolio management services, investment advice as well as the receiving and transmitting of orders pursuant to Article 4 para. 4 no. 1 or no. 2 lit. a or c AIFMG and for whom the exhaustive list of provisions of the Delegated Regulation and WAG 2018 apply in regard to these activities listed in Article 2 para. 3 WAG 2018;[2]

- **Branches of third country firms**, for which, pursuant to Article 23 para. 2 WAG 2018, among others the provisions of Articles 29 to 34 WAG 2018 and Articles 21 to 76 of the Delegated Regulation apply;

- **Investments firms** pursuant to Article 3 WAG 2018 and **investment services providers** pursuant to Article 4 WAG 2018 also fall under the definition of legal entities set out in Article 26 para. 1 WAG 2018 and are therefore also addressed by the organisational requirements contained in the WAG 2018.[3]

The circular provides an overview of the FMA's supervisory practices to the individual aforementioned regulations contained in the WAG 2018 by communicating its legal opinions, while simultaneously aiming to provide the market with guidance about how to comply with the requirements set out in the legal regulations. It is necessary to point out that both the FMA as well as the financial market participants are instructed to undertake all necessary efforts to comply with ESMA Guidelines and Recommendations and other measures passed by ESMA resolution (Article 90 para. 1 3rd sentence WAG 2018, Article 16 (3) ESMA-VO[4]). This circular therefore takes into account the ESMA Guidelines with regard to several aspects of the MiFID requirements regarding the compliance function[5], upon which the FMA's supervisory practices are based.

---

2 See also the general organisational regulations set out in Article 10 InvFG 2011, in particular Article 15 InvFG 2011 and Article 61 of Regulation (EU) 231/2013 (the EU AIFM Regulation).

3 The requirement to establish an independent compliance function pursuant to Article 22 of the Delegated Regulation, an independent risk management function pursuant to Article 23 of the Delegated Regulation as well as the requirement of a separate and independent internal audit function pursuant to Article 24 of the Delegated Regulation does not apply to **investment services provider**, see Article 26 para. 2 WAG 2018. **Investment services providers** shall not be required to appoint an officer for the safeguarding of client assets pursuant to Article 43 WAG 2018 (see also Chapter 9).

4 Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority).

5 ESMA Guidelines on certain aspects of the MiFID compliance function requirements of 25 June 2012 (hereafter: ESMA/2012/388).

4. This circular does not constitute a legal regulation. It is intended to serve as guidance and reflects the FMA's legal interpretation. No rights and obligations extending over and above the provisions of the law can be derived from circulars.

5. Where designations used refer to natural persons, the formulation used applies to both genders.

2. LEGAL BASES

6. The following provisions under European and national law as well as ESMA Guidelines form the basis for this circular:

   - Directive 2014/65/EU (MiFID II);[6]
   - Delegated Regulation (EU) 2017/565: (hereafter: the Delegated Regulation);[7]
   - The Securities Supervision Act 2018 (WAG 2018; Wertpapieraufsichtsgesetz 2018)[8] as well as the FMA regulations issued in relation to it (including the Cross-Selling Regulation);
   - ESMA Guidelines on certain aspects of the MiFID compliance function requirements of 25 June 2012 (ESMA/2012/388, hereafter the ESMA GLs).

3. PRELIMINARY REMARK

7. In addition to an independent compliance function as defined in Article 22 (2) of the Delegated Regulation and Article 29 WAG 2018 (Chapters 5 and 6), an independent risk management function pursuant to Article 23 of the Delegated Regulation and Article 32 WAG 2018 (Chapter 10) as well as an internal audit function that is separate and independent from its other functions and activities shall be established and maintained pursuant to Article 32 WAG 2018 (Chapter 11). The circular hereafter addresses the substantive design of the individual functions.

6 Directive 2014/65/EU of 15 May 2014 of the European Parliament and of the Council on markets in financial instruments (MiFID II) and amending Directive 2002/92/EC and Directive 2011/61/EU.

7 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

8 Federal Law Gazette I No. 107/2017.

4. PRINCIPLE OF PROPORTIONALITY

8. To take into consideration the diversity of the business activities of the legal entities with regard to their size, the focuses of their business and the risk situation, in applying individual organisational rules (such as Article 21 (1), Article 22 (1) and (4), Article 23 (2), Article 24 of the Delegated Regulation) organisational simplifications may be made use of in accordance with the principle of proportionality dependent on the nature, scope and complexity and of the business activities conducted and the nature and scope of investment services and activities performed by the legal entity.

9. Legislators assume that the individual organisational functions have been separated on the basis of the postulation of independence. With respect to the general organisational requirements pursuant to Article 21 of the Delegated Regulation in conjunction with Article 29 paras. 1 and 2 WAG 2018 as well as to the individual functions set out in Articles 22 to 24 of the Delegated Regulation as well as Article 32 WAG 2018, the principle of proportionality is to be considered on a case-by-case basis.

10. Making use of the principle of proportionality (and the simplifications associated with it) must therefore be evaluated and justified separately for each of the individual functions set out in Articles 22 to 24 of the Delegated Regulation. The evaluation may lead to the result, that making use of the principle of proportionality (and associated organisation simplifications) in individual cases is not permissible due to the nature and/or scale and/or complexity of the business activity.

11. In this context it should be clarified that the permanent establishment of an independent compliance function pursuant to Article 22 (2) of the Delegated Regulation is not, however, subject to the principle of proportionality. This basic requirement shall be required to be implemented by every legal entity.

12. Every legal entity shall be required of its own accord to evaluate the application of the principle of proportionality for its specific business model and to present and document this in a plausible way and manner towards the FMA. Provided that the legal entity arrives at the result that making use of the waiver in accordance with the first sentence of Article 22 (4) Delegated Regulation is justified, the legal entity must also additionally judge whether

the effectiveness of the compliance function is compromised. This assessment must be reviewed regularly.[9]

13. In particular the following criteria may be applied:

4.1. NATURE, SCOPE AND COMPLEXITY OF BUSINESS ACTIVITIES

14. Criteria or indicators in relation to the business activities as a whole of the legal entity:
    - which business activities are carried out altogether (also those not related to the provision of investment services); consideration of corporate goals and strategies, interaction between the securities business and other business activities carried out by the legal entity;
    - number of employers;
    - balance sheet and revenue ratios; balance sheet total, profit on ordinary activities.
15. Criteria or indicators in relation to the business activities of the legal entity in conjunction with the provision of investment services and activities:
    - Net result from commission of the legal entity from securities transactions or investment services as well as other revenue in relation to the provision of investment services, investment activities and ancillary services;
    - Client structure with regard to the categorisation of clients pursuant to the WAG 2018: retail clients, professional clients, suitable counterparties;
    - exchange-listed clients;
    - Nature of the sales model: number of employed sales agents, number of sales offices, number of tied agents etc.;
    - Nature of the product portfolio offered: standardised, structured and/or high-risk products, e.g. derivative products, products with margin obligations, obligations to make additional contributions, complex financial instruments, etc.;
    - proprietary issuances, issuance support, volume of proprietary issuances, connection to Wiener Börse;
    - activity as specialist/market maker;
    - organisational level of IT: mapping of statutory requirements with regard to the obtaining of and onward transmission of information in IT systems, IT-supported advice procedures and/or control functions;

[9] Article 22 (4) 3rd sentence Delegated Regulation.

- complete or partial outsourcing of individual operational tasks, and taking on of operational tasks from other companies;
- the legal entity's cross-border services: activity under the freedom to provide services or to provide services through branch establishments.

4.2. NATURE AND SCOPE OF THE INVESTMENT SERVICES AND ACTIVITIES PROVIDED

16. Criteria and/or indicators in relation to the nature of the investment services and activities provided:

- What specific investment services and/or activities are being rendered: receiving and transmitting of orders and/or also investment advice and portfolio management? Are execution-only services provided?
- What is the scope of the individual investment services and/or activities carried out (both in absolute terms and relative to other business activities)?
- Does the legal entity distribute proprietary financial instruments?
- Does the legal entity offer trading for its own account? Are financial analysis reports drawn up? Does the entity issue or place financial instruments?
- Is a multilateral trading facility (MTF) operated? Is an organised trading facility (OTF) operated?
- Is algorithmic trading conducted or a direct electronic access to exchange operating companies offered?
- Are investment advice and portfolio management services offered using a fully or semi-automatic system ("Robo-Advice")?
- Is independent investment advice provided?
- Are investment services provided together with another service or another product as part of a package or as a condition for the same agreement or package ("cross-selling")?
- What is the proportion of these activities in terms of volume and revenues? What is the percentage of the individual WAG-relevant transactions in relation to the legal entity’s other activities (e.g. credit business)? Are they just a secondary activity in the institution’s business model or are the investment services the principle source of revenue for the legal entity?

5. GENERAL ORGANISATIONAL REQUIREMENTS (ARTICLE 21 OF THE DELEGATED REGULATION, ARTICLE 29 PARAS. 1 AND 2 WAG 2018)

17. Pursuant to Article 21 of the Delegated Regulation in conjunction with Article 29 paras. 1 and 2 WAG 2018, legal entities shall comply with a comprehensive set of organisational requirements:

- establishing an organisational structure and maintaining decisionmaking processes that allow the clear documentation of reporting obligations and allocated functions and responsibilities:
  - e.g. organisation charts, department and job descriptions. the allocation of responsibilities and the reporting lines established within the company must be documented systematically and be transparent at all times; in this context, informal responsibilities based on common practice shall be avoided and adjustments and updates shall be made in a timely manner in the course of organisational restructurings;
- ensuring that all relevant persons pursuant to Article 1 no. 65 WAG 2018 are familiar with the procedures that need to be followed in order to properly fulfil their responsibilities:
  - e.g. sufficiently specific, written documentation about the precautions defined for compliance with legal requirements (in the form of rule books such as operating procedures or similar) and measures for informing staff members (e.g. trainings).
- ensuring, establishing and maintaining adequate internal control mechanisms:
  - e.g., approval and authorisation systems, in particular the dual control principle, rules concerning the power to negotiate, separation of responsibilities and functions, as well as physical access restrictions.
- employing personnel with the skills, knowledge and experience necessary to fulfil the tasks:[10]

[10] See also Chapter 6.1.2 (Qualifications) below.

- e.g. targeted recruiting, training schedules and mentoring, orientation by experienced co-workers, job rotation, etc.

- establishing an internal reporting system:
  - e.g. establishment of a formal internal reporting and information system (procedure descriptions, minutes etc.), including transparent documentation obligations.
- maintaining adequate and systematic records of its business activities and internal organisation:
  - e.g. minutes, rule books, job descriptions, order execution channels, asset allocation, etc.;
- ensuring the orderly, fair and professional performance of tasks even if relevant persons perform multiple functions:
  - e.g. organisational and other measures for effectively managing conflicts of interest; restrictions for taking on several functions.[11]

18. The aforementioned obligations are general requirements for the internal organisation and that are to be guaranteed by every legal entity at all times. Only the actual organisational level may be defined on a case-by-case basis and is dependent on the nature, scale and complexity of the legal entity's business activities as well as on the nature and scale of the investment services and activities carried out.[12]

19. In addition legal entities shall establish the following pursuant to Article 21 and Article 26 of the Delegated Regulation:

- systems to safeguard the security, integrity and confidentiality of information:
  - e.g. to ensure that no information is lost, that information can be reproduced accurately and fully within a reasonable period of time, that such information is only accessible to persons cleared for the respective level of confidentiality, and that it is protected against being accessed by unauthorised third parties; particular confidentiality requirements regarding insider information as defined in Article 7 of Regulation (EU) 596/2014 (MAR) in conjunction with Article 119 para. 4 of the Stock Exchange Act 2018 (BörseG 2018; Börsegesetz 2018);
  - safeguarding mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data tampering and

11 See Chapter 6.2 (Independence of the Compliance Function) below.
12 See Chapter 4 (Criteria for the Principle of Proportionality) above.

unauthorised access and to prevent information leakage, so that the confidentiality of the data can be guaranteed at all times. (Article 29 WAG 2018);

- adequate precautions to guarantee the continuity and regularity of investment services and activities (Article 29 para. 3 WAG 2018; Article 21 (3) of the Delegated Regulation):
  - Availability of an emergency management system including the identification of time-critical processes and resources, as well as the impact of failure of business processes or the unavailability of resources (Business Impact Analysis), risk assessments and contingency plan strategies;
  - Defining contingency plans for the restoration and/or continuation of critical processes, ensuring the reproducibility of data or information as well as alternative solutions or minimum required substitute resources;
  - Amending of contingency plans as required; ensuring the necessary consistency between contingency plans and ongoing changes affecting the entity.
- effective and transparent procedures for the immediate handling of complaints from retail clients and their management; storage of records in relation to complaints and the measures taken or to be taken to resolve them, monitoring of procedural steps for handling complaints;
- Creating a risk-based monitoring program.[13]

20. The adequacy and effectiveness of the systems created in accordance with Article 21 (1) and (2) of the Delegated Regulation, of the internal control mechanisms and precautions are to be monitored, regularly assessed, and the measures taken to address any deficiencies (Article 21 (5) of the Delegated Regulation).

[13] Article 22 (2) of the Delegated Regulation.

6. ORGANISATION AND TASKS OF THE COMPLIANCE FUNCTION (ARTICLE 22 OF THE DELEGATED REGULATION, ARTICLE 29 WAG 2018)

6.1. ORGANISATIONAL REQUIREMENTS FOR THE COMPLIANCE FUNCTION[14]

21. When determining the appropriate personal and other resourcing of the compliance function the legal entity must take into account the nature and scope of its investment services and activities and ancillary services. Furthermore it shall grant the staff members of the compliance function with the necessary powers for effectively performing their duties, and grant them access to all information about the provided investment services and activities and ancillary services that is relevant.[15]

22. The personnel requirements that are required for the performance of duties of the compliance function are particularly dependent on the nature, scope and complexity of the investment services and activities and ancillary services performed by the legal entity. In the event of a significant expansion of the activities performed by business units, the legal entity should ensure that the compliance function is also extended commensurately taking into consideration the modified compliance risk. The senior management should monitor regularly whether the number of staff is still adequate for the fulfilment of the duties of the compliance function.[16]

23. In addition to human resources, sufficient IT resources should be allocated to the compliance function.[17]

24. Where budgets are allocated by the legal entity for the individual functions or units, than the compliance function should be provided with a budget that is commensurate to the entity's compliance risk. The compliance officer should be consulted prior to the budget being

[14] See MN 11 above: the permanent establishment of an independent compliance function is not subject to the principle of proportionality.
[15] cf. ESMA Guidelines MN 43.
[16] cf. ESMA Guidelines MN 45.
[17] cf. ESMA Guidelines MN 46.

defined. All decisions relating to larger budget reductions should be documented in written and justified in detail.[18]

25. The whole management body is responsible for the establishment of an independent compliance function and monitors its effectiveness. This responsibility also extends to outsourced activities and processes and also exists in the case that duties are delegated.[19]

26. The significance of the compliance function should be reflected in its position in the entity's organisation.

27. The compliance officer is to be appointed and dismissed[20] by the senior management.[21]

    In the case of credit institutions of significant relevance as defined in Article 5 para. 4 BWG the FMA must be notified about the appointment of a compliance officer pursuant to Article 22 (3) (b) of the Delegated Regulation as well as any change in their person without delay (within 2 weeks) following the appointment.[22] The following information in particular must be submitted to the FMA in this notification[23].

    - Confirmation of internal fitness and propriety check[24],

18 cf. ESMA Guidelines MN 47.

19 See Chapter 7 (Outsourcing).

20 Article 22 (3) (b) Delegated Regulation. See also the Standard Compliance Code of the Austrian Banking Industry (Module 1 - Principles of orderly compliance) item 5 independence.

21 Article 22 (3) b) of the Delegated Regulation uses the term "management body". The definition of the term in the second sentence of Article 4 (1) (36) of Directive 2014/65/EU states the following: Where this Directive refers to the management body and, pursuant to national law, the managerial and supervisory functions of the management body are assigned to different bodies or different members within one body, the Member State shall identify the bodies or members of the management body responsible in accordance with its national law, unless otherwise specified by this Directive. Ultimately in accordance with Article 1 no. 55 WAG 2018 the management body is responsible for the appointment of the compliance officer under Austrian law.

22 Article 73 para. 1b no. 4 BWG prescribed the obligatory **notification of the compliance officer** or any change in their person **pursuant to Article 22 (3) (b) of the Delegated Regulation in credit institutions of significant relevance pursuant to Article 5 para. 4 BWG**. Where credit institutions are obliged pursuant to Article 39 para. 6 no. 2 BWG, to establish a permanent, effective and independently functioning compliance function, they may establish their organisational structure in such a way that the same persons or the same organisational units are competent or responsible for the different compliance functions (see the explanatory remarks about Article 39 paras. 5 and 6 BWG the Annexes to the stenographic accounts of the meetings of the National Council no.106, 26th legislative period).

23 Regarding the submission of the necessary documentation, reference is made to Annex 1 of the FMA-Fit & Proper Circular. Where the Head of the Compliance Function pursuant to Article 39 para. 6 no. 3 BWG is also responsible for the function of the compliance officer pursuant to Article 22 (3) b) of the Delegated Regulation, the required documentation for the notification pursuant to Article 73 para. 1b nos. 2 and 4 BWG only needs to be submitted once to the FMA.

24 Confirmation that a positive check has been conducted about the suitability of the person in question pursuant to the institution's internal policy and procedures for the assessment of the suitability of such persons; cf. FMA-Fit&Proper Circular, MN 154. The documentation about the outcomes of the bank's internal Fit & Proper Assessment must be submitted to the FMA upon request.

- Curriculum Vitae,[25]
- Criminal record certificate[26],
- Sworn declaration regarding the non-existence of reasons for exclusion in Article 39 para. 6 no. 3 in conjunction with Article 5 para. 1, nos. 6 and 7 BWG[27]
- Current organisation chart.[28]

28. For credit institutions that fall below the significance threshold set forth in Article 5 para. 4 BWG, the FMA reserves the right to also request the notification of the new appointment or change in person of a compliance officer.[29]

29. Outsourcings of the compliance function are also to be notified promptly to the FMA.[30]

30. Separate forms are available on the FMA's Incoming Platform for the notification of the appointment of the compliance officer pursuant to Article 22 (3) b) of the Delegated Regulation and the submission of documentation in relation to this as well as for notification of outsourcing of the compliance function.[31]

31. The compliance officer reports to the senior management and acts independently and is not bound by instructions in the performance of his/her tasks.[32]

32. The management body must clearly determine, which of its members is responsible for the monitoring and adherence to the legal entity's organisational requirements. The division of material duties must be documented and kept up-to-date.[33]

---

25 Curriculum Vitae containing the details stipulated in the Annex of the FMA - Fit&Proper Circular 5.1 - 5.5.
26 Cf. in this regard FMA-Fit&Proper Circular, Annex 1 point 8.
27 Cf. in this regard FMA-Fit&Proper Circular, Annex 1 point 6.
28 Cf. in this regard FMA-Fit&Proper Circular, Annex 1 point 9.
29 EBA/GL/2017/12, Guideline 177.
30 Cf. in this regard Article 25 para. 5 BWG, which states that the intended outsourcing of material tasks in relation to banking operations is to be notified in writing prior to the conclusion of an outsourcing agreement. This also includes the outsourcing of the compliance function in accordance with WAG 2018 and the Delegated Regulation. The outsourcing of individual tasks of the compliance function is subject to notification requirements, when the task(s) in question is/are to be qualified as being material as defined in Article 25 para. 5 BWG. For more detailed explanations about the topic of outsourcing see Chapter 7.
31 With regard to the notification about the Head of the Compliance Function pursuant to Article 73 para. 1b no. 2 BWG we refer to the FMA-Fit & Proper Circular (Chapter VII).
32 See also Chapter 6.2 (Independence of the Compliance Function).
33 cf. Article 25 (1) of the Delegated Regulation.

33. Pursuant to Article 22 (3) (b) of the Delegated Regulation, the compliance officer is responsible for the compliance function as well as of preparing activity reports to be presented to the management board and the supervisory board.

34. The legal entity has to ensure that a written activity report is received both yearly by the management body (Article 25 (2) of the Delegated Regulation) as well on a regular basis by the supervisory board (Article 25 (3) of the Delegated Regulation [in the FMA's opinion at least once a year]).

35. The management body also has the right to request information from the compliance officer about the compliance function and about any shortcomings in the company at any time. The compliance officer has an ad hoc information requirement towards the management body and the chairperson of the supervisory board[34], in the case that the compliance function identifies a significant risk.[35] The holding of regular "Jour Fixe" meetings is useful for allowing the exchange of information between the management board and the compliance officer.

36. The employees of the compliance function shall have access to all relevant proprietary information systems and as appropriate to all internal or external audit reports or other reports submitted to the senior management or the supervisory body, in order to ensure that they have a continuous overview about the various units in the entity, in which sensitive or compliance-relevant information might occur. Where necessary the compliance officer and his/her deputy should also be allowed to participate at the meetings of the senior management or the supervisory body. Where this right is not granted, this should be documented and explained in writing. The employees of the compliance function should have thorough knowledge of the organisation, corporate culture, and the decision-making process of the legal entity, in order to be able to determine at which meetings participation is necessary.[36]

---

34 Article 22 (3) (c) of the Delegated Regulation obliges reporting on an ad hoc basis to the "management body". In accordance with the prescribed definitions in Directive 2014/65/EU (in Article 4 (1) (36)) "management body" means the body or bodies of an investment firm (...), which was/were appointed in accordance with national law, which are empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include persons who effectively direct the business of the entity. |Where MiFID II refers to the management body and, pursuant to national law, the managerial and supervisory functions of the management body are assigned to different bodies or different members within one body, the Member State shall identify the bodies or members of the management body responsible in accordance with its national law, unless otherwise specified in MiFID II.

35 Article 22 (3) (c) Delegated Regulation.

36 cf. ESMA Guidelines MN 48 2nd to 5th sentence.

37. The legal entity should ensure that the compliance functions performs its tasks and responsibilities on a permanent basis. The legal entities should therefore establish adequate arrangements for ensuring the responsibilities of the compliance officer are fulfilled when the compliance officer is absent, and adequate arrangements to ensure that the responsibilities of the compliance function are performed on an ongoing basis. The relevant arrangements should be determined in writing.[37]

38. In order to be able to ensure that legal requirements regarding the compliance function are observed, as a minimum deputisation in the case of the absence of the compliance officer must be established. Doing so is intended to ensure that the tasks of the compliance function are permanently fulfilled, even in the absence of the compliance officer. The deputy compliance officer must possess adequate expert knowledge and qualifications, in order to be always to satisfy this requirement.

39. The tasks, competences and powers of the staff members of the compliance function must be determined in writing in the organisational and operating procedures of the legal entity. Information about the monitoring programme and the reporting obligations of the compliance function should also be included, as well as information about the risk-based approach regarding the monitoring activity of the compliance function. In the case of relevant amendments to legal provisions such organisational and operating procedures should be amended without delay.[38]

6.1.1. COMPETENCES

40. To ensure that compliance employees are guaranteed access to information that is relevant to the performance of their duties at all times, the legal entity shall ensure, as defined in Article 22 (3) (a) of the Delegated Regulation, that they are granted access to all relevant databases as well as being granted comprehensive inspection, access and information rights.[39]

41. In order to ensure that compliance staff have the authority required for their duties, the senior management should support them in the exercise of these duties. Authority implies possessing the necessary expertise and relevant personal skills, and may be enhanced by

[37] cf. ESMA Guidelines MN 53.
[38] cf. ESMA Guidelines MN 55.
[39] cf. ESMA Guidelines MN 48 1st sentence.

the legal entity's compliance strategy (i.e. the legal entity's cross-functional planning of the compliance goals that are to be achieved) explicitly acknowledging the specific authority of the compliance staff.[40]

6.1.2. FITNESS AND PROPRIETY

42. The staff members of the compliance function must at least be familiar with MiFID II, the accompanying delegated acts (e.g. Delegated Regulation (EU) 2017/565) and the corresponding legal provisions in the WAG 2018, as well as FMA Regulations issued in relation to WAG 2018 and all accompanying ESMA Standards and Guidelines[41], where they are relevant for the performance of their tasks. Compliance function staff members must be regularly trained to keep their knowledge up-to-date. The compliance officer must be more-highly qualified.[42]

43. The compliance officer should have sufficiently broad knowledge and experience and a sufficiently high level of expertise so as to be able to assume responsibility for the compliance function as a whole and ensure that it is effective.[43]

44. It is necessary against this background to ensure that the compliance officer possesses the necessary knowledge about the processes and procedures that exist in his company, as well as about the products and services offered.

45. The compliance officer must also possess at least a basic knowledge about how algorithmic trading systems and trading algorithms work, in the case that the legal entity operates such trading systems.[44]

46. The compliance officer should have obtained the necessary professional experience to be in a position to be able to judge compliance risks and conflicts of interest, that arise from the legal entity's business activities. Such experience may have been gained in operational positions, in other control functions or in regulatory functions.[45]

---

40 cf. ESMA Guidelines MN 49.
41 See MN 138 et seq. of the FMA-Fit & Proper Circular as well as EBA/GL/2017/12 about the specific requirements for the Head of the BWG Compliance Function.
42 cf. ESMA Guidelines MN 50 1st and 2nd sentences.
43 cf. ESMA Guidelines MN 44.
44 Article 27 WAG 2018.
45 cf. ESMA Guidelines MN 51.

47. In this context it is necessary to refer to the level of expertise set out in Article 22 (3) (a) of Delegated Regulation (EU) 2017/565[46], which persons entrusted with compliance functions shall be required to have, and to also mentioned that at least the compliance officer should either have gained relevant prior professional experience as an employee of, for example, a trading or treasury department, in the compliance department, in the internal audit or similar, or can be trained up to the position of compliance officer by means of specific training and education programmes in the field of compliance as well as by means of job rotations within the company and practical workshops as a compliance expert.

48. In light of the fact that the specific expert knowledge required may vary depending on the business model of the legal entity due to the differing compliance risks that are faced, a newly employed compliance officer may therefore need to gain additional specialised expert knowledge focused on the specific business model of the legal entity even if they were previously the compliance officer of another legal entity.[47]

49. In order to ensure current knowledge in relation to the developments in the securities market, as well as keeping abreast of any statutory and legal changes, it is particularly important that the compliance officer completes ongoing further training.

50. In this context it should be noted that the EBA/ESMA Joint Guidelines on the assessment of the suitability of members of the management body and key function holders[48] also addresses the heads of internal control functions, which also includes the compliance officer (incl. the Head of the BWG Compliance Function).[49]

51. The checking of the professional qualification and the personal reliability of the compliance officer shall be conducted by way of an internal fit and proper assessment when the compliance officer is newly appointed or where there is a change in their person.[50] The nature and scale of the internal Fit & Proper assessment may be defined by the legal entity itself, but must observe the principle of proportionality, so that the nature, scale and complexity of the activities as well as the undertaking's risk structure is adequately taken into consideration. The documents gathered for the internal Fit & Proper Assessment as well as the process of assessment of suitability as well as its outcome must be documented,

46 Reference is also made to Article 21 (1) (d) of the Delegated Regulation.
47 cf. ESMA Guidelines MN 52.
48 EBA/GL/2017/12. The Guidelines set minimum requirements regarding the assessment of the personal reputation, professional suitability and experience of employees holding so called key functions.
49 Cf. also the FMA-Fit & Proper-Circular
50 Cf. also the FMA-Fit & Proper-Circular, Chapter VI ("Internal Bank Fit&Proper Assessment and Policies").

and be made available to the FMA at the FMA's request.[51] Furthermore, the FMA also has the possibility on an ad hoc basis to conduct its own Fit & Proper test for compliance officers.

6.2. INDEPENDENCE OF THE COMPLIANCE FUNCTION

52. In accordance with Article 22 (2) of the Delegated Regulation, every legal entity is required to establish and maintain a permanent independent compliance function, that monitors the adequacy and effectiveness of the measures prescribed to avoid breaches of the legal rules set out in the Delegated Regulation as well as WAG 2018, and regularly assesses them, as well as providing support for the competent divisions of the undertaking that is responsible for investment services. This obligation is not subject to the principle of proportionality, which means that an independently operating compliance function must be established in any case.

53. While the whole management body shall be responsible for the establishment of an orderly compliance organisation and for the monitoring of the effectiveness of such an organisation[52], although the compliance function performs its tasks independently of the management body and other units within the legal entity. In particular, the legal entity should ensure that other business units are not permitted to issue instructions to compliance staff or to otherwise exert influence on their activities.[53]

54. If the management body does not following important recommendations or judgments of the compliance function, then the compliance officer should document this and report it in the compliance reports.[54]

55. The method for determining the remuneration of employees involved in the compliance function shall neither be allowed to compromise their objectivity nor be suited to do so (Article 22 (3) (e) of the Delegated Regulation).

56. The remuneration structure shall be designed in such a way that the salary of the compliance staff is not related to the earnings of individual corporate divisions monitored by

51 See also MN 277 regarding the requirement to submit Fit & Proper documentation in the case of the new appointment of a compliance officer or a change in their person in credit institutions as defined in Article 5 para. 4 BWG.
52 cf. Article 25 (1) of the Delegated Regulation.
53 cf. ESMA Guidelines MN 58.
54 cf. ESMA Guidelines MN 59.

the compliance function, as in that case it may be possible that the compliance tasks may no longer be able to be carried out independently and objectively under certain circumstances due to financial incentives. The remuneration structure should instead be based on performance-based pay based on qualitative rather than exclusively quantitative criteria and/or a higher base salary from the start with a small proportion of variable components.[55]

6.2.1. COMPATIBILITY OF FUNCTIONS

57. In practice the issue of compatibility of functions and activities arises frequently (e.g. the compliance officer is also the anti-money laundering officer, a member of the risk management function or a similar control function, or an employee in the legal department or the internal audit). It may be assumed in principle that employees who deal with compliance issues shall not be allowed to take over any other activities (principle of separation of functions). To ensure the independence of the compliance function therefore requires a separation of the compliance function from the operative business units in the form of separating those monitoring from those monitored. As a result, employees involved in the compliance function are solely to focus upon compliance agendas, and the performing of activities or services in particular those on the market side (e.g. providing advice, being active in trading activities either for customers or proprietary trading, etc.) is as a rule not permitted.

58. If the analysis of the business activities[56] finds that the investment services or investment activities provided by the legal entity are classified as less complex and extensive, then Article 22 (4) of the Delegated Regulation sets out an option to deviate from the requirements set out in Article 22 (3) (d) and (e) of the Delegated Regulation where several functions are performed by one and the same employee and with the remuneration structure of a staff member entrusted with compliance agendas in accordance with the principle of proportionality.

59. In this context the considerations why any case of anyone performing multiple functions (making use of the principle of proportionality) appears appropriate with regard to any

[55] cf. FMA Circular on the problem of conflicts of interest in relation to certain systems of remuneration taking into account the ESMA Guidelines "Remuneration policies and practices (MiFID)" of 02.04.2014 as well as [ESMA/2013/606] MN 17 among others. The circular related to the legal basis under MiFID and is currently being revised.

[56] See Chapter 4 (Criteria for the Principle of Proportionality).

conflicts of interest of any nature or adequate resources for performing duties are to be documented and submitted to the FMA upon request (Article 22 (4) of the Delegated Regulation).

60. Provided that the legal entity arrives at the result that making use of the waiver in accordance with the Article 22 (4) of the Delegated Regulation is justified, the legal entity must also judge whether the effectiveness of the compliance function is compromised. This assessment must be reviewed regularly by the legal entity and make available to the FMA upon request by the FMA (Article 22 (4) third sentence of the Delegated Regulation).

61. A legal entity may for example fall under the exemption rule, if full-time position is not necessary for compliance tasks due to the nature, scale and complexity of its investment services and activities and ancillary services offered.[57]

62. While a compliance officer must be named in any case, the deployment of a compliance officer who is solely deployed in this position may be disproportionate for smaller legal entities with a very narrow range of activities.

63. A material condition for the compatibility of several functions is that in any case, by performing multiple functions that the independence of the compliance function is not compromised, and that adequate resources are available for the orderly fulfilling of the respective areas of responsibility.

64. If employees who are responsible for compliance agenda are also involved in other activities, the legal entity must justify this in a transparent manner and prove to the FMA (by means of accurate documentation regarding the reason for the decision, information about other activities that the employee in question also performs) to what such a mixed role is justified taking into account proportionality criteria.

65. Where the legal applies such an exemption, then conflicts of interest that arise between the different areas of responsibility of the person in question are to be avoided to as great an extent as is possible.[58]

66. Furthermore the legal entity shall regularly check, whether the justification for such an organisational simplification continues to exist or whether an adjustment of the organisational concept is required, (e.g. due to the expansion of the business area).

[57] cf. ESMA Guidelines MN 63.
[58] cf. ESMA Guidelines MN 64.

67. The relevant simplifications may be permissible in the case of the deputy compliance officer under consideration of the principle of proportionality pursuant to Article 22 (4) of the Delegated Regulation where the appropriate conditions exist. In this case too, the conflicts of interest that arise between the different areas of responsibility of the person in question are to be avoided to as great an extent as is possible.

68. It must be ensured in every case, also where there is a justified reason for organisational simplifications, that the compliance function performs the duties that it is responsible for without hindrance. This shall be presented and documented to the FMA in a transparent way.

6.2.1.1 COMPLIANCE FUNCTION & EMPLOYEES IN THE INTERNAL AUDIT FUNCTION

69. Pursuant to Article 24 of the Delegated Regulation and Article 32 WAG 2018, a legal entity shall establish and maintain an internal audit function that is separate and independent from its other functions.[59]

70. In the case of credit institutions that do not fulfil the size criterion set out in Article 42 para. 6 BWG and which therefore do not require a separate organisational unit that is responsible for internal audit duties, but whose business activities are predominantly in the field of investment services, shall consider the establishment of an independent internal audit function as defined in Article 24 Delegated Regulation, with the principle of proportionality[60] taken into account.[61]

71. In light of the fact that the internal audit function also has to monitor the orderly fulfilment of duties of the compliance function, a combination of these functions is generally to be avoided due to self-auditing being forbidden.

72. A combination of these functions is therefore only possible in practice on a very restricted basis, and in such cases coordination with the FMA with reasons being given being an expedient way to proceed.

73. Where use is made of the exemption, then the legal entity must ensure that both functions are properly discharged i.e. soundly, honestly and professionally.[62]

74. In order to comply with the ban on self-checking, the necessary organisational precautions must be taken for any (permissible) combination of functions. Such precautions must be defined and ensured accordingly by the legal entity. In the case of simultaneously performing the compliance function and that of the internal audit, with regard to the fact that the internal audit function is also required to check that the duties of the compliance function are conducted in an orderly manner, and consequently in light of the ban on self-checking has to prescribe that the compliance agendas are checked by an employee of the legal

---

59 See also Article 42 para. 6 BWG in this regard. In the case of credit institutions which under the provisions of the BWG have adequate independent risk management function and internal audit, the tasks specified in Articles 23 to 24 of the Delegated Regulation may be performed by the relevant organisational unit. (cf. Article 25 para. 3 WAG 2018).

60 cf. ESMA Guidelines MN 69.

61 cf. ESMA Guidelines MN 69.

62 cf. ESMA Guidelines MN 69.

entity, who has received the necessary specialist training, or by an external third party (e.g. the external auditor or the auditing association).

75. When making use of simplifications the reasoning must be comprehensively documented by the legal entity. The FMA will, if necessary, review within its ongoing supervisory activities to what extent the performance of the compliance function by an employee of the internal audit function is proportionate in the specific case in hand.

6.2.1.2 COMPLIANCE FUNCTION & ANTI-MONEY LAUNDERING OFFICER, EMPLOYEES OF THE RISK MANAGEMENT FUNCTION OR SIMILAR CONTROL FUNCTIONS

76. The combination of the compliance function with other control units (e.g. prevention of money laundering, risk management function) may be permissible, provided that doing so does not have an adverse influence of the effective and comprehensive performance of duties and the independence of the compliance function. The reasons justifying the combining of such functions should be documented in a transparent manner, so that the FMA may assess whether the combination of the functions is justified under the given circumstances.[63]

77. The person who is appointed as the person responsible for the safeguarding of client assets (Article 43 WAG 2018), may also perform other control functions (e.g. compliance officer).[64]

78. It is also generally permissible for the complaints management function to also be taken over by the compliance function.[65]

6.2.1.3 COMPLIANCE FUNCTION & LEGAL DEPARTMENT

79. A legal entity that is subject to simplified requirements under the principle of proportionality in relation to Article 22 (3) (d) and (e) of the Delegated Regulation, may combine the legal department and the compliance function.[66]

80. In the case of the compliance function being linked to the legal department particular caution is to be taken in relation to any conflicts of interest that might occur. Furthermore, the directly

63 cf. ESMA Guidelines MN 67 2nd and 3rd sentences.
64 See also recital 5 of Delegated Directive (EU) 2017/593.
65 Article 26 (3) of the Delegated Regulation.
66 cf. ESMA Guidelines MN 65.

reporting line to the management body must be maintained and the compliance function must be provided with adequate resources and competences by the legal entity.

81. Where use is made of such a simplification on the basis of the principle of proportionality, then the justification for doing so must be documented in a transparent matter. The FMA will, during its ongoing supervisory activities, if necessary review to what extent the performing of the compliance function by the legal department is proportionate with regard to the specific case in hand.[67]

6.2.1.4 COMPLIANCE FUNCTION & MEMBER OF THE MANAGEMENT BOARD/EXECUTIVE DIRECTOR

82. The performance of the compliance function by a member of the management board or an executive director is only permissible in exceptional cases, since the law stipulates that the compliance function has reporting requirements towards the management body or the executive director on the one hand, and the management body on the other hand appoints the compliance officer, has full responsibility for the compliance function and monitors its effectiveness.[68]

83. The simultaneous performance of both functions may be permissible under certain circumstances, A legal entity may for example fall under the exemption rule, if a full-time position is not necessary for compliance tasks due to the nature, scale and complexity of the legal entity's business and the nature and scale of its investment services and activities offered.[69]

84. In the case of microenterprises (as a guide: 6 full-time equivalent employees), taking into consideration the principle of proportionality, under certain circumstances the compliance function may be performed by a member of the senior management or the management board, such as in the case that the distribution of functions is difficult in terms of resources due to an extremely limited headcount, and due to the high level of involvement of the member of the senior management or the management board of microenterprises does not appear expedient. [70]

---

67 cf. ESMA Guidelines MN 66.
68 See in particular Article 25 of the Delegated Regulation.
69 ESMA Guidelines MN 64 on the criteria relating to the performance of multiple functions other than the specific examples listed.
70 See Chapter 4 (Criteria for the Principle of Proportionality) above.

85. In the event that the same person performs both the compliance function and the function of a member of the senior management or the management board, the legal entity shall have to ensure that the member of the senior management or the member of the management board is able to dedicate sufficient time to fulfil all the obligations associated with the compliance function. Furthermore the director who simultaneously also performs the compliance function, is not allowed, in the interests of ensuring its independence or to avoid conflicts of interest to be responsible for the marketing division.

86. The legal entity should notify the FMA without due delay of the compliance function being performed by a member of the senior management or a member of the management board, and in the notification also justify and prove to what extent in the specific case in hand it is justified for a member of the senior management or a member of the management board to be performing the compliance function under consideration of proportionality.

87. The FMA will, if necessary, review within its ongoing supervisory activities to what extent the performance of the compliance function by a senior manager or a member of the management board is justified in the specific case in hand.

6.2.2. OTHER REQUIREMENTS

88. In order to avoid any unnecessary duplications and/or to exploit potential synergies within the company, the compliance officer should co-ordinate their tasks stipulated in the Delegated Regulation or WAG 2018 with other organisational units (e.g. internal audit, risk management, legal department) and refer to these units' work results (e.g. audit results) when performing compliance tasks. It is sensible to co-ordinate audit activities to be performed in the field of compliance with other organisational units, e.g. the internal audit (e.g. reciprocal exchanging of information concerning audit findings).[71] In this case, a written and comprehensive set of organisational and operating procedures that fulfil the requirements set out in Article 21 (1) of the Delegated Regulation shall be drawn up, which also include the clearly allocation competences assigned to individual business areas.

89. The audit procedures to be undertaken by the compliance function should not be solely based on the audit procedures of the internal audit function.

[71] cf. ESMA Guidelines MN 16.

90. In any case, the compliance function shall ensure that it coordinated the statutory duties for which it is responsible. The exploitation of such a synergy shall not be allowed to result in the compliance function being undermined to such an extent the specific agendas or activities as defined in Article 22 of the Delegated Regulation can no longer be performed to any extent by the compliance officer.

6.3. RISK ASSESSMENT

91. The legal entity shall ensure that the compliance function pursues a risk-based approach in the interest of an efficient deployment of resources. For this purpose, starting with an evaluation of the compliance risk, focuses should be determined for the monitoring and advisory activities of the compliance function. This risk assessment should be performed regularly, so that the focus and the scope of compliance monitoring and advisory activities always corresponds with current requirements (Article 22 (2), first subparagraph of the Delegated Regulation).[72]

92. In so doing, the compliance function should identify the scope of the legal entity's compliance risk, taking into consideration the investment services and activities and ancillary services provided by the legal entity as well as the types of financial instruments traded and distributed by the legal entity.[73]

93. When assessing the compliance risk, the applicable obligations from the Delegated Regulation and WAG 2018 as well as the policies, procedures, systems and controls are to be taken into consideration that the legal entity implements in the area of investment services and activities. Furthermore the assessment should also include the findings from monitoring activities and any relevant internal or external audits.[74]

94. The risk assessment forms the basis for the objectives and work programme of the compliance function. The results of the risk assessment shall be reviewed regularly as well as, when required on an ad hoc basis, in order to capture any emerging risks (e.g. those results from new business fields or other restructuring within the entity).[75]

---

72 cf. ESMA Guidelines MN 14.
73 cf. ESMA Guidelines MN 15.
74 cf. ESMA Guidelines MN 16.
75 cf. ESMA Guidelines MN 17.

95. In order to identify the potential risks of non-compliance with the Delegated Regulation as well as WAG 2018 within the company, each legal entity is required to define internal procedures which ensure a specific continuous assessment of the legal entity's business activities and a systematic recording of all obligations pertaining to the legal entity under WAG 2018. The assessment or capturing shall allow the legal entity to derive the corresponding compliance risks and to make them reviewable. In this context, it needs to be considered from which activities and/or which persons (not only employees but also clients) compliance risks may arise in the first place.

6.4. MONITORING PROGRAMME AND MONITORING ACTIVITIES (ARTICLE 22 OF THE DELEGATED REGULATION)

96. The compliance function shall ensure, by conducting regular risk-based monitoring activities, that the defined measures, strategies and procedures (i.e. organisational and operating procedures) for the prevention of or for discovering compliance risks within the legal entity are complied with.

97. The compliance function shall conduct such activities on an ongoing basis and not only when particular circumstances exist. To do so, regular monitoring on the basis of a monitoring programme is required. All key areas of investment services and activities should be regularly by covered in the monitoring activities taking into account the compliance risk of the associated with the respective business areas. The compliance function should therefore be in a position to respond rapidly to unforeseen events, and if required to change the focus of its activities within a short timeframe.[76]

98. The compliance function shall draw up a risk-based monitoring programme that covers all areas relating to the legal entity's investment services and activities as well as relevant ancillary services. On the basis of the assessment of the compliance risk in relation to the risk assessment, priorities should be determined for the monitoring programme to ensure the comprehensive monitoring of the compliance risk. Relevant information that was collected in relation to the monitoring of the handling of complaints, must also be included in the monitoring programme.[77]

[76] cf. ESMA Guidelines MN 56.
[77] Article 22 (2) 2nd subparagraph Delegated Regulation.

99. The aim of a monitoring programme should be to evaluate whether the legal entity's business is conducted in compliance with its obligations arising from the Delegated Regulation or under WAG 2018 and whether its internal guidelines, organisation and control measures remain effective and appropriate.

100. The risk-based approach to compliance should form the starting point for determining the appropriate tools and methodologies, as well as the extent of the monitoring programme and the frequency of monitoring activities performed by the compliance function (either on a recurring, ad-hoc and/or continuous basis). Furthermore, the compliance function should ensure that its monitoring activities are not solely limited to file-based or computer-based monitoring procedures. I should also verifies how policies and procedures are implemented in practice, for example by means of on-site inspections conducted at the operative business units. The compliance function should also determine the scope of reviews to be performed.[78]

101. Suitable measures and procedures for the monitoring activities of the compliance function include:[79]

(a) the use of aggregated risk measurements (for example, risk indicators, i.e. parameters that are in a position to be able to predict changes in the risk profile; see also the criteria when applying the principle of proportionality);
(b) submission of reports for attention by the management, in which there are material deviations between the actual occurrences and expectations are documented (exceptions report) or situations requiring resolution (issues log);
(c) targeted surveillance of trading, observation of procedures, desk reviews and/or interviews with the responsible staff members.[80]

102. The monitoring programme should reflect any changes to the legal entity's risk profile, which may arise, for example, from significant events such as corporate acquisitions, changes to the IT system, or re-organisation. It should also extend to the implementation and effectiveness of any remedial measures taken by the investment firm in response to breaches against the provisions contained in the Delegated Regulation or WAG 2018 as

78 cf. ESMA Guidelines MN 21.
79 cf. ESMA Guidelines MN 27.
80 cf. ESMA Guidelines MN 22.

well as the Regulations of the FMA issued based upon WAG 2018, to be monitored in accordance with the monitoring programme.[81]

103. In conducting its monitoring activities, the compliance function should take the following into account:

(a) the obligation of the respective business area to comply with regulatory requirements;
(b) the first level controls in the legal entity's business areas (i.e. controls by the operative units, as opposed to second level controls performed by the compliance function);
(c) reviews by the risk management function, the internal control function, the internal audit function or other control functions in the area of investment services and activities.[82]

104. The checks conducted by other control bodies should be coordinated with the monitoring measures of the compliance function, however, in so doing respecting the independence and the mandates of the different functions.

105. The compliance function must be involved in the monitoring of the handling of the complaints procedure. It is important in so doing to consider that complaints can form a source of valuable information for its general monitoring activities. In this context the legal entity should provide access to the compliance function in connection with all customer complaints.[83]

106. The compliance function must be involved in the reviewing of the internal product governance process and must regularly check the product governance arrangements and their development.[84]

6.5. REPORTING OBLIGATIONS OF THE COMPLIANCE FUNCTION

107. Pursuant to Article 22 (2) (c) in conjunction with Article 22 (3) (b) of the Delegated Regulation, the compliance officer shall submit a written activity report at least once a year

81 cf. ESMA Guidelines MN 23.
82 cf. ESMA Guidelines MN 24.
83 cf. ESMA Guidelines MN 26.
84 Article 30 para. 8 WAG 2018 and Article 31 para. 10 WAG 2018;

to the management bodies (i.e. the management board and the supervisory board[85]). It depends on the organisational structure of each company whether this report is forwarded to the supervisory body by the management board or by the compliance officer.

108. Such reports should contain a description of the implementation and effectiveness of the general control measures in relation to investment services and activities as well as an overview of the identified risks and the necessary measures that have been taken or are intended to be taken. They should be drawn up at suitable intervals, but as least annually. In the event that material shortcomings are identified by the compliance function, then the compliance officer should also inform the management body without delay.

109. The written compliance report to be sent to the management bodies should relate to all business units, that are involved in the provision of investment services and activities and ancillary services. In the event that the activities of the legal entity are not fully covered, then this should be clearly justified in the report.[86]

110. The written compliance reports should, where relevant, in particular contain the following:[87]

(a) a description of the implementation and effectiveness of the general control measures in relation to investment services and activities;
(b) an overview of the major findings of the review of policies and procedures;
(c) and summarised depiction of the on-site inspections conducted by the compliance function or file reviews, including the gaps and shortcomings discovered in the organisation of the company and the compliance procedure, as well as suitable measures taken in this regard;
(d) Risks that were identified during the monitoring activity of the compliance function;
(e) the material changes and further developments with regard to the legal requirements that have arisen during the reporting period as well as the measures that have been taken or are intended to be taken, in order to ensure compliance with the altered legal requirements (in the case that the senior management was not already advised of this by other means);
(f) other significant compliance problems, that have occurred since the last report;

85 Article 22 (2) (c) of the Delegated Regulation obliges reporting on an ad hoc basis to the "management body". See the definition of the term defined in Article 4 (1) (36) of Directive 2014/65/EU (MiFID II)
86 cf. ESMA Guidelines MN 28.
87 cf. ESMA Guidelines MN 29.

(g) information about the designed financial instruments and the distribution strategy within the product governance process;
(h) information about the products offered or recommended by the legal entity and the services provided;
(i) information regarding the handling of complaints and the necessary measures;
(j) material correspondence with competent authorities.

111. If the compliance function identifies considerable risks of infringements against the rules set out in the Delegated Regulation and WAG 2018 by the legal entity, then the compliance function shall inform the management bodies (i.e. the management board and the supervisory board[88]) on an ad hoc basis and submit a report. The report should also contain proposals for necessary remedial measures.[89]

112. The compliance function should clarify whether additional reporting lines are necessary to other compliance functions within the group.[90]

6.6. ADVISORY DUTIES OF THE COMPLIANCE FUNCTION

113. The legal entity must ensure that the compliance function fulfils its advisory obligations, including providing support for staff training, day-to-day assistance for staff and participating in the drawing up of new policies and procedures within the legal entity.[91]

114. The legal entity should develop and promote a "compliance culture" throughout the entire entity. Its purpose should not only be to establish the overall environment in which compliance matters are treated, but also to engage staff with the principle of improving investor protection.[92] The creation of a "compliance culture" is first and foremost the duty of the management body. The "top at/from the top" is decisive for this purpose, although not sufficient in its own right, i.e.. the understanding of compliance-related issues must be transported into all areas of the company, and must also be subscribed to by the employees.

88 Article 22 (3) (c) Delegated Regulation.
89 cf. ESMA Guidelines MN 30.
90 cf. ESMA Guidelines MN 31.
91 cf. ESMA Guidelines MN 33.
92 cf. ESMA Guidelines MN 34.

115. The legal entity must ensure that its employees are sufficiently well trained. The compliance function should support the business units responsible for investment services and activities (i.e. all employees who are either directly or indirectly involved in the provision of investment services and activities) in drawing up training plans and the execution of training measures. At this juncture it is also particular necessary to refer to the qualifications of client advisors, the existence of which the legal entity must prove to the FMA upon request (Article 55 WAG 2018).[93]

116. Trainings and other support should primarily, but not exclusively, be focused on the following[94]:

(a) internal criteria and procedures of the legal entity and its organisational structure in the area of investment services and investment activities;
(b) Requirements in particular those set out in the Delegated Regulation, other relevant EU Regulations, WAG 2018 and other relevant FMA Regulations or Circulars, relevant ESMA publications (in particular Guidelines and Q&As) as well as other significant requirements of a regulatory or supervisory law basis as well as any amendment to these conditions.

117. The employee trainings should be held regularly and as necessary also on an ad hoc basis. They should to oriented towards the respective target group, i.e. being focused accordingly as required to all staff members, individual business areas or individual staff members. Furthermore, the content of such training should be updated and amended in a timely manner in the event of there being relevant legislative amendments (e.g. new legal regulations, new standards or ESMA Guidelines as well as ESMA publications, changes to the legal entity's business model) or developments regarding the legal entity's business model.[95]

118. The compliance function should periodically assess whether staff in the area of investment services and activities hold the necessary level of awareness and correctly apply the legal entity's policies and procedures.[96]

---

93 See also the "Guidelines for the assessment of knowledge and competence" issued on 22 March 2016 (ESMA/2015/1886 EN) and the FMA Circular on the "Criteria for the Assessment of Knowledge and Competence of Investment Advisors and Persons providing Information about Investment Products (Article 55 WAG 2018)" of 21 August 2017.
94 cf. ESMA Guidelines MN 35.
95 cf. ESMA Guidelines MNs 36 and 37.
96 cf. ESMA Guidelines MN 38.

119. Furthermore, the compliance function should also provide assistance to staff from the operative units in their day-to-day business and be available to answer questions arising out of daily business activity.[97] This means that an important advisory and support function is provided by the compliance function with regard to measures to be taken regarding the observance of legal provisions or internal policies.

6.7. INVOLVEMENT OF THE COMPLIANCE FUNCTION IN PROCESSES

120. The legal entity shall ensure that the compliance function is involved in the legal entity's development of policies and procedures in relation to investment services, activities and ancillary services. The compliance function should therefore have the opportunity, to provide specialist compliance knowledge and advice to business units in relation to strategic decisions, new business models, new products or new advertising strategies in the area of investment services and activities. If recommendations of the compliance function are not heeded, then the compliance function should document this, and present this in its compliance reports.[98]

121. The legal entity shall ensure that the compliance function is involved in any significant modifications of the organisation of the investment firm in the area of investment services, activities and ancillary services. This also applies to the decision-making process about the approval of new business areas or financial products. The compliance function should therefore be given the right to participate in the approval process for financial instruments to be taken up in the distribution process. The senior management should ensure that the compliance function is involved in the aforementioned decision-making processes of the operative business units and is therefore able to fulfil its advisory role.[99] Furthermore the compliance function should be incorporated in the product governance process and shall monitor this pursuant to Article 30 para. 8 and Article 31 para. 10 WAG 2018.[100]

122. It is crucial in terms of the proactive participation of the compliance function in minimising potential violations of the obligations under the WAG 2018 or the Delegated Regulation, to integrate the compliance officer into as many information and reporting processes as

97 cf. ESMA Guidelines MN 39.
98 cf. ESMA Guidelines MN 40.
99 cf. ESMA Guidelines MN 41.
100 cf. also MN 107.

possible. The compliance function monitors the processes for the handling of complaints.[101] . It is not necessary to involve the compliance function in an operative manner (in relation to the processing of complaints) over and above their general monitoring duty.[102]

123. It is necessary that the compliance function is involved in among other cases in the checking of marketing communications, processes in relation to the introduction of products, as well as investment advice and portfolio management processes, is involved in the setting of the principles in relation to investment services as well as in the accompanying approval procedures[103] and similar processes, so that it has as much information as possible for the assessment of compliance risks.[104] In this regard the compliance function should be or is required to be involved in the following internal processes:

- approval of the principles on remuneration (Article 27 of the Delegated Regulation);
- drawing up of investment research as per the definition of Article 36 of the Delegated Regulation;
- reviewing of the best execution policy;
- independent investment advice / non-independent investment advice (including regulating of inducements);
- product development and product distribution (product governance process Articles 30 and 31 WAG 2018);
- investment advice and portfolio management processes;
- marketing communications, information on costs and charges;
- complaints process: reviewing of information regarding complaints and their handling, (Article 26 (7) of the Delegated Regulation) as well as the monitoring of processes for the handling of complaints as well as taking into account complaints as being a source of relevant information (Article 22 (2) (d) of the Delegated Regulation).
- monitoring of recording and retention obligations for telephone calls and electronic communication;

101 Article 22 (2) (d) Delegated Regulation.
102 For more detailed statements regarding complaints management see Chapter 8 (Complaints management).
103 Article 27 (3) of the Delegated Regulation.
104 See also Chapter 6.3 (Risk assessment) above.

- monitoring of compliance with the requirements regarding algorithmic trading systems and trading algorithms (Article 2 Delegated Regulation (EU) 2017/589);
- Incorporation into the audit process with regard to the knowledge and competence of investment advisors and persons providing information about investment products [ESMA Guidelines for the assessment of knowledge and competence" issued on 22 March 2016 (ESMA/2015/1886 EN)].[105]

124. The legal entity shall ensure that the compliance function is involved in all material non-routine correspondence with competent supervisory authorities in the area of investment services and activities.[106]

7. PARTIAL OR COMPLETE OUTSOURCING OF THE COMPLIANCE FUNCTION OR INDIVIDUAL ACTIVITIES

125. Pursuant to Article 34 WAG 2018 in conjunction with Article 30 et seq. of the Delegated Regulation critical or important operational functions may be outsourced to third parties.[107]

126. An operational function shall be considered as critical or important pursuant to Article 30 para. 1 of the Delegated Regulation, where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU (MiFID II), or its financial performance, or the soundness or the continuity of its investment services and activities.

127. The establishing an independent compliance function as well as equipping it with the necessary powers, resources and expertise necessary for the orderly performance of tasks shall lie in the direct responsibility of the senior management.[108] Related to this is

[105] See also the "Guidelines for the assessment of knowledge and competence" issued on 22 March 2016 (ESMA/2015/1886 EN) and the FMA Circular on the "Criteria for the Assessment of Knowledge and Competence of Investment Advisors and Persons providing Information about Investment Products (Article 55 WAG 2018)" of 21 August 2017.

[106] cf. ESMA Guidelines MN 42.

[107] Where the investment firm and the service provider are members of the same group, the investment firm may, for the purposes of complying with this Article and Article 32, take into account the extent to which the firm controls the service provider or has the ability to influence its actions, Article 31 (4) of the Delegated Regulation.

[108] See Chapter 6.1 above.

the obligation to take organisational precautions to prevent the misuse of inside information, to monitor the transactions carried out by employees and other relevant persons, and the obligation in general to carry out investment services and activities in accordance with the Delegated Regulation and WAG 2018. These tasks shall be considered important as defined in Article 30 (1) of the Delegated Regulation.

128. The possibility exists in relation to outsourcing, to outsource the compliance function or individual tasks of the compliance function to third parties.

129. The outsourcing of the compliance function shall be considered as outsourcing of material operational banking tasks as defined in Article 25 para 5 BWG. The outsourcing of individual tasks of the compliance function or other intended outsourcing of investment services and activities as defined in WAG 2018 are subject to notification requirements, when the task(s) in question is/are to be qualified as being material as defined in Article 25 para. 5 BWG. Article 25 para. 5 BWG prescribes that credit institutions are obliged to notify the FMA in writing without delay about the intended outsourcing of material tasks in relation to banking operations prior to conclusion of an outsourcing agreement.[109]

130. The FMA has made a separate notification form available on the Incoming Platform for the notification of the outsourcing of the compliance function.[110]

131. In the case of outsourcing, the responsibility for the fulfilment of the legal requirements of the compliance function shall nevertheless in all cases remain with the senior management of the institution that is outsourcing, and shall not lead to a delegation of the duties of the senior management (Article 31 (1) (a) of the Delegated Regulation).

132. The outsourcing of important operational functions shall not be allowed to be undertaken in such a way that materially impairs the quality of internal control or the ability of the FMA to monitor the firm's compliance with all obligations. Furthermore, pursuant to Article 31 (2) (h) of the Delegated Regulation the service provider shall co-operate with the competent authority for the outsourcing institution in relation to the outsourced functions.

---

[109] Within the FMA supervisory reform package (published in Federal Law Gazette I no. 149/2017) a legal basis was introduced into the Austria Banking Act (Article 25 BWG and the Annex to Article 25 BWG) for the outsourcing of material tasks for banking operations. The outsourcing of the compliance function pursuant to Article 22 (2) of the Delegated Regulation is generally qualified from the FMA's point of view as an important outsourcing subject to notification requirements.

[110] The notification form for intended outsourcings pursuant to Article 25 para. 5 BWG is to be used for such notifications.

The outsourcing institution, its statutory auditor and the respective competent authorities shall actually have access to the data in relation to the outsourced functions, as well as to the premises of the service provider, provided that this is necessary for the purposes of ensuring effective supervision pursuant to Article 31 (2) (i) of the Delegated Regulation.

133. The full or partial outsourcing of the compliance function (such as within a group, or within a sector to the central institution or leading institution, or to another institution in the affiliation of institutions or to a third party [service provider]) does not lead to a delegation of the original compliance responsibility of the management board of the institution that outsources these tasks. In specific cases a centralised group compliance function may however lead to a better access to information for the compliance function and permit the function to work more efficiently, above all if the members of the group share the same premises.[111] Where the outsourcing institution and the service provider belong to the same group[112], the outsourcing institution may take into account pursuant to Article 31 (4) of the Delegated Regulation for the purpose of fulfilling Articles 31 and 32 of the Delegated Regulation, to what extent it controls the service provider or is able to influence its actions.

134. The establishment of the compliance function and the appointment of a compliance officer are management tasks of the senior management that may not be delegated and may not be outsourced. In the case of a complete or partial outsourcing of compliance agenda a contact person for compliance tasks shall still be named at the legal entity outsourcing these agendas.[113]

135. The requirements on the contact person for compliance issues within the outsourcing legal entity shall be lower in accordance with their activity as a contact person than for a compliance officer. The contact person should in any case be in the position, to understand the enquiries of the management board or the employees to compliance issues. Furthermore, the contact person must hold adequate qualifications to be able to review the activities performed by the service provider, and as necessary to scrutinise them. Furthermore the contact person shall also be placed at the disposal of the senior management, staff members as well as the supervisor in relation to compliance issues.

111 cf. ESMA Guidelines MN 78.
112 As defined in Article 25 para. 4 BWG.
113 With regard to the performing of additional activities by the contact person for compliance issues please refer accordingly to the remarks in Chapter 6.2.1 (Compatibility of Functions).

136. In the case of outsourcing in the area of the performance of the compliance function or individual compliance-related tasks, economic considerations (cost management) should not (exclusively) play a role, but such a consideration should also serve to ensure and improve the quality of compliance in the company.

137. In cases where a legal entity, due to the nature, size and scope of its business activities, is unable to employ compliance staff, who are independent of the performance of services they monitor, then outsourcing of the compliance function is likely to be an appropriate approach to take.[114]

138. The legal entity shall ensure that the compliance officer also performs his activities in an independent manner even in the case that the compliance function is outsourced.[115]

139. Prior to the selection of the service provider, the legal entity should conduct a due diligence assessment to guarantee that Article 29 WAG 2018 and Article 34 WAG 2018. The legal entity should ensure that the service provider possesses all legally prescribed authorisations as well as the necessary competence, expertise, capacity, adequate resources and suitable organisational structures as well as access to all information that is relevant for the service provider, in order to be able to perform the outsourced duties of the compliance function in an orderly and effective manner. The extent of the due diligence assessment is dependent on the nature, scale, complexity and risk of the tasks and processes that are outsourced.[116] The legal entity should also continue to ensure the permanence of the compliance function in the event of a partial or complete outsourcing of the compliance function, by convincing itself of the ability of the service provider to perform this function on a continuous basis rather than only performing it when specific circumstances prevail.[117] The service provider must be in a position to perform the activities of the compliance function on a continuous basis and not only on an ad hoc basis.

140. Furthermore, the outsourcing institution shall ensure pursuant to Article 31 (2) (l) of the Delegated Regulation that the continuity and quality of the outsourced tasks or services is maintained even in the event of the termination of the outsourcing. Pursuant to

114 cf. ESMA Guidelines MN 79.
115 cf. ESMA Guidelines MN 74: the requirements for the compliance function are not affected by having been outsourced, and include independence and not being subject to instructions.
116 cf. ESMA Guidelines MN 75.
117 cf. ESMA Guidelines MN 76.

Article 31 (2) (g) of the Delegated Regulation the outsourcing institution must be in the position where applicable to also be able to terminate its outsourcing agreement with immediate effect, where doing so is in the interest of the client. In the written agreement between the outsourcing institution and the service provider, pursuant to Article 31 (3) of the Delegated Regulation, the corresponding rights and obligations of the parties to the contract must be clearly determined. In particular the outsourcing institution retains its instruction and termination rights, its information rights as well as its rights of inspection of and access to the books and premises of the service provider and furthermore it shall be ensured in the written agreement that a further outsourcing by the service provider shall only be allowed to occur with the written approval of the outsourcing institution (Article 31 (3) of the Delegated Regulation).

141. The legal entity shall monitor in an effective manner whether the service provider is performed in an orderly manner, both in terms of quality and quantity, and shall control the risks associated with outsourcing in an appropriate manner. The management body shall be responsible for the ongoing oversight and monitoring of the outsourced function, and must pursuant to Article 31 (2) (e) of the Delegated Regulation possess the necessary expert knowledge and resources for doing so, in order to be able to effectively monitor the outsourced tasks, and to control such risks. The senior management may appoint a specific person to supervise and monitor the outsourced function on their behalf.[118]

[118] cf. ESMA Guidelines MN 77.

8. COMPLAINTS MANAGEMENT

142. Reference is made to Article 26 of the Delegated Regulation in this context, according to which a legal entity is required to define effective and transparent strategies and procedures for complaints management and to permanently implement them, which are used to handle complaints by clients or potential clients without delay.[119]

143. The legal entity shall accordingly establish a complaints management function, that is responsible for the reviewing of complaints. This function may be conducted by the compliance function[120]. The formal resolving of complaints, may from the FMA's point of view also be conducted by another body (e.g. the specialist division in question). It is however important that the complaints management function assumes ultimate responsibility for the substantive checking of complaints, i.e. the complaints management function shall in any case undertake the reviewing of the complaints, and in this regard be involved in the complaints handling process. In the event that the substantively handling of the resolving of a complaint is carried out by another body, then the complaints management function shall in particular review, whether it is substantively adequate.

144. An effective handling of complaints only exists from the FMA's point of view (as previously set out in Article 17 para. 5 WAG 2007), if the complaint is not processed by the person about whose performance the client is complaining. This is particularly the case due to the associated conflict of interest. An appropriate handling of complaints requires among other things that complaints are processed by persons that were not directly involved in the incident being complained about, i.e. under no circumstances by the competent advisor. This specifically means that the competent body shall not also be allowed to be the originator or subject matter of the complaint.[121]

145. The term complaint is to be broadly understood.[122] It does not only address material claims (e.g. claims for damages) but also those which are unauthorised from the perspective of

119 Article 26 (1) of the Delegated Regulation.

120 Recital 38 in combination with Article 26 (3) of the Delegated Regulation, as well as Chapter 6.2.1.2 (Combining of functions).

121 Federal Administrative Court 29.07.2014, Case no. W107 2000396-1/9E.

122 For a definition of the term complaint, see also, among other sources Article 5 para. 1 no. 4a of the Regulation on Asset, Income and Risk Statements (VERA-V; Vermögens-, Erfolgs- und Risikoausweis-Verordnung) and well as the Guidelines for complaints-handling for the securities (ESMA) and banking (EBA) sectors, JC/2014/43.

the legal entity or whose content has not (yet) been reviewed. It is not in any case permitted to flatly refuse certain topics addressed by the complaint handling function to be established by the legal entity. Every complaint should therefore be documented and reviewed by the competent body.

146. It is also not permissible that a specific (in terms of the amount involved) threshold ("de minimis threshold") is defined for the involvement of the complaint handling.

147. With regard to the handling of complaints the legal entity shall define a binding written regulation (in the form of operating procedures or an internal guideline), which clearly defines the procedure for handling complaints, the competences and standards for the timely processing of complaints.

148. For an effective and expedient complaint handling procedure it is also necessary to have a regular and systematic evaluation, about the results of which the senior management should be informed.

149. The legal entity shall inform about its complaints handling procedure in an easily accessible manner (e.g. in brochures, leaflets, contract documents or on its website). The client (as per the definition in Article 1 no. 34 WAG 2018) must be informed about any other necessary documents with regard to a complaint as well as the competent body or person at the legal entity for handling complaints. The client must also be informed about the handling process (processing timeframe, the legal entity's stance regarding the complaint, alternative dispute resolution bodies etc.). The legal entity shall make this information available in a clear, precise and up-to-date manner.[123]

9. OFFICER FOR THE SAFEGUARDING OF CLIENT ASSETS

150. The legal entity shall transfer complete responsible for the fulfilling of the provisions regarding the safeguarding of client financial instruments and funds to a single officer (Article 43 WAG 2018). The single officer should possess sufficient skills and authority in order to discharge duties effectively and without impediment, including the duty to report to the legal entity's senior management in respect of oversight of the effectiveness of the

[123] Article 26 (4) and (5) Delegated Regulation.

firm's compliance with the safeguarding of client assets requirements. This person may also perform other control functions, provided that it is ensured that he/she is able to fulfil his/her obligations in relation to the safeguarding of client financial instruments and funds effectively. This function may also be conferred upon the compliance function.[124]

10. RISK MANAGEMENT (ARTICLE 23 OF THE DELEGATED REGULATION IN CONJUNCTION WITH ARTICLE 32 WAG 2018)

151. Pursuant to Article 23 of the Delegated Regulation and Article 32 WAG 2018, a legal entity[125] shall define risk management guidelines and procedures, take effective measures to control the risks and establish a permanent and independent risk management function.[126] The obligation to establish an independent risk management function pursuant to Article 23 of the Delegated Regulation is subject to the principle of proportionality.[127] Where the establishment of an independent risk management function is not proportionate or is unnecessary on the grounds of the nature, scope and complexity of the business activities conducted as well as on the basis of the nature and scope of the investment services and activities provided by the legal entity, the grounds for making use of the exceptions must be proven. In this context, an risk assessment of the company is required in order to identify the risks inherent to the individual transactions, procedures and systems and/or to define how to address or manage these risks.[128]

152. For credit institutions, the BWG serves as the primary reference document with regard to the establishment of risk management function. Article 39 BWG shall apply, which stipulates the control, monitoring and limitation of all risks pertaining to banking business and banking operations. If an organisational unit in a credit institution is entrusted with the risk management function, which satisfies the requirements of the Delegated Regulation

124 Article 7 Delegated Directive (EU) 2017/593 as well as recital 5 thereof.

125 The provisions of Articles 3, 21 to 25, 28 to 31, 33, 34, 44 to 53, 57 and 59 of the Delegated Regulation as well as Articles 33, 36, 45 to 55, 58, 60, 90, Article 92 paras. 9 and 10 and Articles 94 to 96 shall apply to insurance undertakings that conduct the mediation of units in investment funds pursuant to Article 6 para. 3 VAG 2016 in relation to this activity; where such insurance undertakings have a compliance function, risk management function and an internal audit function in accordance with the provisions of the VAG, the duties listed in Articles 22 to 24 of the Delegated Regulation may be conducted by the relevant organisational unit (Article 2 para. 2 WAG 2018).

126 Pursuant to Article 26 para. 2 no. 2 WAG 2018 investment services providers shall only be exempted from the establishment of an independent risk management function. Para. 3 shall therefore also apply to these undertakings.

127 See Chapter 4 (Criteria for the Principle of Proportionality) above.

128 See Chapter 6.3 (Risk Assessment) above.

and WAG 2018 with regard to its independence, it shall not be necessary to establish another independent organisational unit that carries out the risk management tasks pursuant to Article 23 of the Delegated Regulation in conjunction with Article 32 WAG 2018. The underlying risk management policy, however, shall be evaluated with respect to the requirements of Article 23 of the Delegated Regulation in conjunction with Article 32 WAG 2018 (risks arising from best execution, from sales models for securities, etc.) and adapted or extended as necessary.[129]

153. The annual reporting obligation to the management body arising from Article 23 (2) (b) of the Delegated Regulation may be taken over by the risk management function established in accordance with the BWG. Such reports must in this regard also contain statements regarding whether and in what way the risk management function was conducted in accordance with Article 23 of the Delegated Regulation in conjunction with Article 32 WAG 2018.

[129] See also the EBA "Guidelines on Internal Governance" published on 27.09.2017 (EBA/GL/2017/11), that entered into force on 30.06.2018.

11. INTERNAL AUDIT (ARTICLE 32 WAG 2018 IN CONJUNCTION WITH ARTICLE 24 OF THE DELEGATED REGULATION)

154. Pursuant to Article 24 of the Delegated Regulation, a legal entity[130] shall establish and maintain an internal audit function that is separate and independent from its other functions. This obligation is subject to the principle of proportionality.[131]

155. One of the main tasks of the internal audit function shall be to establish, implement and maintain an internal audit plan. This means that it shall not only carry out audits related to reporting dates but also that the audit-relevant units within the entity shall be constantly considered within the audit planning and shall be audited accordingly. The internal audit function, therefore, plays a significant role, and in addition to the general organisational requirements according to Article 21 of the Delegated Regulation, the tasks carried out by the compliance and the risk management functions shall be audited.[132] This shall contain among other item as comprehensive review of at least all of the significant business areas of the entity on the basis of a risk-oriented approach.

156. Also, compliance with the conduct of business rules of the Delegated Regulation WAG 2018 vis-à-vis clients, such as, for example, client rating, obtaining information from clients ("drafting a client profile"), documentation of advice provided and the processing of client orders shall particularly be audited. Based on the audit results, recommendations shall subsequently be issued, the compliance with these recommendations shall be checked and, at least once a year, a written activity report drawn up containing the measures taken to resolve any shortcomings[133], which shall also be forwarded to the supervisory body.[134]

---

130 For insurance undertakings that perform the brokering of investment fund units pursuant to Article 6 para. 3 VAG 2016, with respect to this activity the provisions set out in Articles 3, 21 to 25, 28 to 31, 33, 34, 44 to 53, 57 and 59 of the Delegated Regulation as well as Articles 33, 36, 45 to 55, 58, 60, 90, Article 92 paras. 9 and 10 and Articles 94 to 96 WAG 2018 shall apply; provided that such insurance undertakings have an suitably independent risk management function and an internal audit function in accordance with the provisions of the VAG 2016, the duties listed in Articles 22 to 24 of the Delegated Regulation may be performed by the respective organisational unit (Article 2 para. 2 first sentence WAG 2018).

131 See Chapter 4 (Criteria for the Principle of Proportionality) above.

132 Federal Administrative Court (VwGH) 30.01.2015, Ra 2014/02/0116-5.

133 Article 24 (c) in conjunction with Article 25 (2) of Delegated Regulation (EU) 2017/565.

134 Article 25 (3) of the Delegated Regulation. As far as exclusivity, independence and impartiality of the internal audit function are concerned, reference is also made to the principles set out the FMA Minimum Standards for Internal Auditing of 18 February 2005 (FMA-MS-IR).

157. The duties of the internal audit function pursuant to Article 24 of the Delegated Regulation in conjunction with Article 32 WAG 2018 may be performed in credit institutions by an internal audit function established pursuant to Article 42 BWG. If certain size-related criteria are met, Article 42 para 6 BWG stipulates the mandatory establishment of a separate organisational unit for the internal audit function. Based on the reference to Article 26 para. 3 WAG 2018 to the BWG, this unit may therefore perform the duties of the internal audit.

158. Those credit institutions that do not fulfil the size-related criteria set out in Article 42 para. 6 BWG and therefore do not have at internal audit function in accordance with the BWG, but whose business activities are prominently in the field of investment services, shall therefore check about the establishment of an independent internal audit function as defined in Article 24 of the Delegated Regulation, taking into consideration the principle of proportionality.

159. The independence of the internal audit function shall be ensured especially in organisational terms. In this context, it must be ensured that the independence of the internal audit function is not being restricted with respect to its tasks (independence in preparing the internal audit plan), reporting obligations (directly to the management bodies, i.e. management board and supervisory board), and competences (no restriction of access to information).

160. With regard to the combination of functions and/or the other performance of multiple functions by employees of the internal audit function, the following must be observed:

161. The internal audit function shall generally operate separately and independently from the compliance and risk management functions as well as the function of the anti-money laundering officer[135], since it is the internal audit function's responsibility to check the other functional units and, in the event that functional units are combined, and the issue of self-audit would otherwise arise.[136]

135 See also the "FMA Circular on the Anti-Money Laundering Officer" MN 29 et seq.
136 See Chapter 6.2.1.1 (Compliance Function & Employees in the Internal Audit Function) above for further statements.