FMA

Document No.: 01 / 2020
Publication date: 02.01.2020

FMA MINIMUM STANDARDS

FOR INTERNAL AUDITING

(FMA-MS-IR)

TABLE OF CONTENTS

All English translation of the authentic German text is unofficial and serves merely information purposes. All translations are prepared with great care, but linguistic compromises may have to be made. The reader should also bear in mind that some legal provisions mentioned in this circular will remain unclear without certain background knowledge of the Austrian legal and political system. Please note that the cited legal provisions are subject to change in the future.

Translator's Notes to assist in reading of these Minimum Standards:

Executive directors are always members of the management body in its management function (i.e. the management board).
Non-executive directors are always members of the management body in its supervisory function (i.e. the supervisory board).
Management body implies both the management board and the supervisory board.

I. INTRODUCTORY REMARKS

(1) These Minimum Standards do not constitute a legal regulation. They serve as **guidance for credit institutions and financial institutions** and reflect the FMA's legal interpretation and the FMA's practical recommendations for conduct. No rights and obligations extending over and above the provisions of the law can be derived from them. The FMA reviews whether legal provisions, especially those is Article 39 paras. 1 and 2 as well as Article 42 of the Austrian Banking Act (BWG) have been breached on a case-by-case basis due to non-observance of recommendations in Minimum Standards. These Minimum Standards replace the Minimum Standards for Internal Auditing issued on 18.02.2005 (No. 01/2005).

(2) Further-reaching requirements for the internal **governance of credit institutions**, including internal audit, are contained in the **European Banking Authority's** (EBA) **"Guidelines on Internal Governance"** (EBA/GL/2017/11, "**IG-GL**"). The IG-GL, which has been applicable since 30.06.2018 addresses competent supervisory authorities and supervised credit institutions in equal measure.[1]

(3) These FMA Minimum Standards shall not prevent **higher standards** from being set by credit institutions. Other FMA Minimum Standards shall remain unaffected.

(4) Within the entire framework of supervisory law, internal auditing is afforded substantial significance. In addition to the supervisory board and the bank auditor, it constitutes an important control body, **and therefore constitutes an important point of contact for the supervisory authority.**

(5) Internal auditing also plays an important role as a control function within the credit institution. The **Three Lines of Defence Model**[2] states that risks should be addressed and managed on three levels. While the **business lines** – the *first line of defence* - should identify and manage risks that they encounter within the scope of their activities, the risk management function, as the *second line of defence* should identify, measure, monitor and report about risks across departments. The **BWG compliance function** pursuant to Article 39 para. 6 BWG, the **WAG[3] compliance function** pursuant to Article 22 (2) of Delegated Regulation ("Del Reg") (EU) 2017/565 and the **function of the anti-money-laundering officer(s)** in accordance with Article 23 para. 3 FM-GwG[4] are also components of the *second line of defence*. It is the role of **internal audit function** as the *third line of defence* to conduct audits for all departments, processes, procedures and systems on both a regular and an ad hoc basis, and to inform the management body as well as the competent supervisory body about how effective the governance

[1] Pursuant to Article 69 para. 5 BWG as well as Article 16(3) of Regulation (EU) No 1093/2010 ("EBA Regulation"), when performing its duties, the FMA shall take **European convergence in respect of supervisory tools and supervisory procedure** into account. For this purpose, **the FMA shall participate in the activities of EBA** and **apply Guidelines**, Recommendations, Standards and other measures passed by EBA. It has not been possible to implement the requirements for the composition of the nomination committees (independent members) due to the explicit statutory amendment required to do so. Consequently, the FMA had to submit a declaration of partial non-compliance to EBA in light of this.

[2] Basel Committee on Banking Supervision Guidelines, Corporate governance principles for banks, 2015.

[3] Securities Supervision Act 2018 ("**WAG**"; Wertpapieraufsichtsgesetz 2018)

[4] Financial Markets Anti-Money Laundering Act ("**FM-GwG**"; Finanzmarkt-Geldwäschegesetz)

framework including the risk management framework is, and that corresponding procedures and principles have been defined and observed on an ongoing basis.

(6) The significance of the internal audit function in particular arises from its **constant presence** in the credit institution, the **ongoing auditing** of all departments, processes, procedures and systems as well as knowledge obtained from doing so. As a internal control function within the institution, it is able to identify risks, threats and deficiencies of the credit institution **before the bank auditor and banking supervision**, and is required to report such findings to the members of the management body, as well as the supervisory board or the competent supervisory body of the credit institution under law or in accordance with its statutes.[5]

II. SCOPE OF APPLICATION AND DEFINITION

(7) These FMA Minimum Standards generally apply to all **credit institutions** that are authorised to perform one or several of the banking transactions listed in Article 1 para. 1 BWG as well as **finance institutions** as defined in Article 1 para. 2 BWG. Under Article 3 para. 1 no. 9 BWG, credit institutions conducting exchange bureau business in accordance with Article 1 para. 1 no. 22 BWG are exempted from the application of Article 42 BWG, and consequently also the application of these Minimum Standards, provided that their cooperation is not required in drawing up the consolidated financial statement of the superordinate credit institution. These FMA Minimum Standards apply also to Austrian credit institutions that are active in other Member States (Article 2 no. 5 BWG) under the freedom to provide services and/or the freedom of establishment (Article 10 BWG). In the case of groups of credit institutions, they also apply to the group internal audit function. Furthermore, they also cover instances of the partial or complete outsourcing of internal auditing tasks.

(8) Pursuant to **Article 77d BWG**, the enforcement of Article 42 BWG only falls exclusively within the FMA's competence where the enforcement of such tasks has not been conferred upon the **European Central Bank (ECB)** pursuant to Regulation (EU) No 1024/2013 (SSM Regulation). Article 4 (1) (e) SSM Regulation lists the ECB's areas of competence, in particular ensuring compliance with the requirements for credit institutions to have robust governance arrangements in place, including internal control mechanisms. In conjunction with Article 6 SSM-R a direct ECB competence therefore arises with regard to the enforcement of Article 42 BWG for "significant institutions" as defined in Article 6 (4) SSM-R. Pursuant to Article 4 (3) SSM-R, the ECB is required to apply relevant Union law. Where this exists in the form of Directives transposed into national law, it shall apply the latter. This means that the ECB directly applies the regulations set out in the BWG with regard to the internal auditing of significant institutions.

[5] In this context Article 32 WAG 2018 and Article 24 of Delegated Regulation (EU) 2017/565 as well as the FMA Circular regarding the organisational requirements of the Securities Supervision Act 2018 and Delegated Regulation (EU) 2017/565 ("WAG 2018 Organisational Circular") paras. 154 ff should also be taken into consideration.

(9) For the purpose of these FMA Minimum Standards, internal auditing shall be understood as the **function** to be set up by credit institutions as legally ordered, which reports directly to the executive directors and which serves the exclusive purpose of ongoing and comprehensive reviews of the legal compliance, appropriateness and suitability of the entire undertaking (Article 42 para. 1 BWG).

III. RESPONSIBILITY OF THE MANAGEMENT BODY IN ITS MANAGEMENT FUNCTION

(10) Credit institutions are required to establish an internal audit function that **reports directly to the members of the management body in its management function (executive directors)** (Article 42 para. 1 BWG).

(11) The responsibility for establishing and ensuring the ability of the internal audit function to function in an orderly manner, including issuing of organisational guidelines, lies with **all members of the management body in its management function collectively**, and may not be delegated. This shall also apply in the case that individual executive directors are assigned specific remits within the credit institution.[6]

(12) All executive directors must permanently ensure with regard to the tasks to be performed by the internal auditing that an **expedient level of organisation** and **adequate quantitative and qualitative resources in terms of human resources and expertise available for the internal audit function** are available, also for covering any special auditing activities.

(13) **Written organisational guidelines** are to be drawn up about internal auditing under the responsibility of the management body in its management function, to be approved by the management body in its management function (c.f. chapter IV.A and para. 130 IG-GL for further detail); the respective current version of such organisational guidelines shall be distributed to all staff members of the credit institution.

IV. GENERAL PRINCIPLES RELATING TO INTERNAL AUDITING

A. ORGANISATIONAL GUIDELINES RELATING TO INTERNAL AUDITING

(14) Internal auditing activities are in particular tied closely to the **organisational guidelines** for the internal audit function. Such organisational guidelines are reviewed on both **a regular basis and an ad hoc basis** with regard to their **adequacy and effectiveness and adapted as required**. They do not restrict the tasks of the internal audit function in accordance with these FMA Minimum Standards in any way.

[6] Instructions relating to internal auditing must be made jointly by at least a minimum of two executive directors (Article 42 para. 3 BWG). Under this provision, at least two executive directors are specifically required to be responsible for internal auditing. Some issues, however, due to their particular significance fall under the responsibility of the management body in its management function in its entirety.

The adaptation of the organisational guidelines for internal auditing takes place under the responsibility of all Ko - and instigated where necessary by the internal audit function.

(15) **In particular**, organisational guidelines shall contain:

a. the definition, objective and significance of internal auditing;

b. the position and organisational integration of internal audit within the credit institution;

c. the organisational structure of internal auditing (including the distribution of competences);

d. principles of internal auditing and its specific design (cf. chapters IV.B to IV.C for further details);

e. the duties of internal auditing and conducting of audit activities by it (cf. for greater detail chapters V and VI);

f. the powers and obligations (especially rights of information and reporting obligations) of the internal audit function (cf. chapters VI.D and VI.F for further details).

B. PERMANENT ACTIVITY

(16) Credit institutions must establish an internal audit function that is solely responsible for auditing the legality, orderliness and expedience of the entity as a whole on a comprehensive and ongoing basis (Article 42 para. 1 BWG).

(17) The internal audit function is therefore **established on a permanent basis,** performing activities throughout the entire year i.e. **on an ongoing rather than only on an ad hoc basis**. Auditing activities should be understood as working through an audit plan, including the option to exercise rights of information at any time and to be able to conduct special audits. The intensity of audit activity depends on the size and nature of the credit institution to be audited, as well as the nature, scale, complexity and risk profile of its business activities.

C. EXCLUSIVITY, INDEPENDENCE AND IMPARTIALITY

(18) The internal audit function performs its tasks independently, objectively and impartially. As a rule, it is therefore **not combined**[7] **with other functions**, especially not other control functions, namely risk management, BWG compliance in accordance with Article 39 para. 6 BWG, WAG compliance in accordance with Article 22 (2) of Delegated Regulation (EU) 2017/565 and the anti-money-laundering officer in accordance with Article 23 para. 3 FM-GwG.

[7] With regard to the combination with the WAG compliance function, see the FMA Circular regarding the organisational requirements of the Securities Supervision Act 2018 and Delegated Regulation (EU) 2017/565 ("WAG 2018 Organisational Circular") of 11.09.2018, paras. 69 et seq.; with regard to the combination with the function of the Anti-Money-Laundering officer see the FMA Circular on internal organisation for the prevention of money laundering and terrorist financing published on 19.03.2019, paras. 33 et seq.

(19) The internal audit function is **not subject to any instruction** in relation to the planning and conducting of audits, reporting, and the evaluations of the outcomes of audits as well as in taking the decision to initiate special audits. This does not affect the right of at least two executive directors to order the conducting of special audits (See Chapter VI.B for further detail).

(20) The staff members in the internal audit function shall generally **only** be active in the internal audit function of the credit institution to be audited, and to be entrusted with such tasks.

(21) Under no circumstances shall staff members of the internal audit function be allowed to audit areas in which they themselves are active (**"Prohibition of self-auditing"**) (cf. IG-GL para. 198), especially also within the scope of group internal audit (cf. chapter VII). Consequently, the internal audit function does not draw up any bank-internal policies and procedures. The internal audit function's staff members are not involved in decision-making or business processes and shall not perform any other tasks that are incompatible with their audit activities.

D. STAFFING IN QUANTITATIVE TERMS

(22) The internal audit function shall be staffed in such a way in duly considering the scope of the institution's business so that it is able to perform its duties as intended (Article 42 para. 1 BWG).

(23) In terms of staffing levels and expertise, the staffing resources of the internal audit function must be adequate in terms of the size and nature of the credit institution to be audited, and in terms of the nature, scale, complexity and risk profile of its business activities, and dimensioned to ensure the internal audit function is able to perform its tasks appropriately (cf. IG-GL para. 197). **Any special audits to be conducted** must also be taken into account. It must in any case be ensured that the internal audit function to function is permanently able to function.

(24) Internal auditing duties must be assigned to a separate organisational unit within the credit institution.[8] This does not apply, pursuant to Article 42 para. 6 BWG, however for credit institutions,

a. whose **total assets** do not exceed **EUR 300 million**; or
b. whose **annual average** number of employees does not exceed **50 full-time employees**; or
c. whose **total assets do not exceed EUR 1 billion**, and which are affiliated to a central institution or belong to a group of credit institutions, where a separate **organisational unit** for internal audit exists **within the sectoral network or the group**, that is equipped and organised with due adherence to Article 42 para. 2 BWG at all times; or
d. whose total assets do not exceed EUR 1 billion, and which are subordinate to an **EU parent credit institution or a parent credit institution in a Member State** pursuant to Article 30 para. 1 nos. 1 to 6 BWG, where a separate organisational unit for internal audit exists within the EU parent credit institution or a parent credit institution in a Member State, that is equipped and organised in accordance with the legal norms and

[8] In this context, it is also necessary to refer to Article 24 of Delegated Regulation (EU) 2017/565.

the supervisory and control options of the FMA and Oesterreichische Nationalbank are not impeded; or

e. whose **total assets do exceed EUR 1 billion**, but which are affiliated to a central institution or belong to a group of credit institutions and have submitted an **application** to the FMA, to be allowed to be exempted from the requirement to establish a separate organisational unit and which was authorised by the **FMA** (Article 42 para. 6 final sentence BWG).

(25) Where the credit institution is affiliated to a central institution or belongs to a group of credit institutions and there is a **sectoral or intra-group organisational unit**, this organisational unit is staffed and organised at all times observing the requirements set forth in Article 42 para. 2 BWG and actually and demonstrably performing the internal auditing tasks for the credit institution.

(26) A **separate organisational unit** is to be understood as a body directly subordinate to the management body in its management function, staffed with at least one staff member working exclusively for the internal audit unit.

(27) Regarding the permissibility (of the extent) of outsourcing pursuant to Article 42 para. 6 BWG, it is necessary to differentiate between the following cases:

a. Where one of the exceptions listed in Article 42 para. 6 nos. 1 and 2 BWG exists, then a separate organisational unit is not required to be established, thereby enabling the full outsourcing of internal auditing.

b. Where a separate organisational unit needs to be established, individual tasks in relation to internal auditing may nevertheless be outsourced.

c. Based on the **special provision set out in Article 42 para. 6 nos. 3 et seq. BWG** a credit institution within a sectoral association or within a group (see MN 24 above c to e) may also fully outsource the internal audit function, although in such instances it may only be outsourced to an organisational unit within the sector or group.[9] It also applies that the organisational unit for the sector or the group itself shall be allowed to outsource individual tasks.

Where internal auditing is fully outsourced on the basis of the waiver and special rules pursuant to Article 42 para. 6 nos. 1 and 2 or no. 3 BWG, general outsourcing provisions contained in Article 25 BWG and the Annex to Article 25 BWG must be observed. Where individual tasks relating to internal auditing are outsourced, a case-by-case review must be conducted about whether Article 25 BWG and the Annex apply.[10]

(28) However, in all cases **ultimate responsibility of the management body in its management function**, especially in relation to the monitoring of observance of the outsourcing agreement, may however never be outsourced.

[9] Paras. 22 and 23 of the EBA Guidelines on Outsourcing (EBA/GL/2019/02) must be observed.

[10] The outsourcing of internal auditing tasks generally indicates the existence of materiality as defined in Article 25 para. 2 BWG. Cf. para. 29b of the EBA Guidelines on Outsourcing (EBA/GL/2019/02) regarding a potential exception from this principle.

E. STAFFING IN QUALITATIVE TERMS

(29) Internal auditing duties shall not be permitted to be entrusted to persons for whom **reasons for exclusion** exist (Article 42 para. 1 BWG)

(30) Circumstances making the orderly performance of internal auditing duties unlikely shall be considered as reasons for exclusion. Reasons for exclusion are deemed to exist, where the person in question **does not possess the requisite expertise and experience in banking** (Article 42 para. 2 no. 1 BWG) and where this might impair the function from being performed objectively (Article 42 para. 2 no. 2 BWG).

(31) Observance of Article 42 para. 2 no. 1 BWG requires that **staff members of the internal audit function** possess an adequate level of theoretical knowledge (necessary expertise) and practical knowledge (necessary experience in banking) for auditing a credit institution.

(32) The up-to-dateness of the **necessary expertise of all staff members** in the internal audit unit will be ensured by appropriate measures.

(33) Specific reasons for exclusion from the internal audit function in accordance with Article 42 para. 2 no. 2 BWG exist where the **objective performance of the function** may be **impaired**.

(34) To ensure that the objective performance of internal auditing tasks and to ensure the objectivity and independence of the bank auditor, in particular **it shall not be permitted, in the case of outsourcing** to appoint **the same natural person concurrently as both bank auditor and internal auditor for the same credit institution** (Article 42 para. 2 no. 2 BWG). Where the bank auditor and the internal auditor belong to the same external auditing company or the same statutory audit institution, internal measures shall be taken to separate both functions and to ensure that both mandates are fulfilled independently, and to ensure a strict separation in personnel and organisational terms between the tasks for bank auditing and internal auditing.

(35) Furthermore, to ensure that internal auditing duties are performed objectively, no reason for exclusion shall be allowed to exist for any staff member of the internal audit function that would apply to the person as bank auditor in accordance with Article 62 nos. 6, 12 and 13 BWG. Article 62 no. 6 BWG relates to the principle of exclusivity (cf. MN 20) as well as prohibiting self-auditing (cf. MN 21). The reasons for exclusion set out in Article 62 nos. 12 and 13 BWG apply in the case of individual tasks of the internal audit unit being outsourced.

(36) The head of the separate organisational unit for the internal audit function established on the basis of legal regulations must be fit and proper in fulfilling the requirements in accordance with Article 42 para. 1 BWG in conjunction with Art. 5 para. 1 nos. 6 and 7 BWG as well as in accordance with Article 42 para. 2 BWG. This means that the requirements for personal suitability (propriety) in accordance with Article 5 para. 1 nos. 6 and 7 BWG shall also apply for the Head of the Internal Audit Function[11] as well as those regarding reasons for exclusion in accordance with Article 42 para. 2 BWG. Special requirements also

[11] Please see the FMA Circular on the assessment of suitability of executive directors, non-executive directors and key function holders (Fit & Proper Circular) published on 30.08.2018 MNs 142-145 regarding the suitability requirements for the Head of the Internal Audit Function.

exist regarding the technical suitability (fitness) of the Head of the Internal Audit Function. Along with in depth theoretical knowledge about internal auditing activities, the Head of the Internal Audit Function must also possess comprehensive practical knowledge of banking, obtained from at least three years activity in the same entity or in another entity of a comparable business type. [12]

V. INTERNAL AUDITING DUTIES

A. BENCHMARKS AND SCOPE OF STATUTORY AUDITS

(37) Checking of legal compliance shall include the ongoing and comprehensive auditing of the entire entity with regard to applicable **laws, regulations and administrative decisions**.

(38) The propriety check in particular covers the **reviewing of the appropriateness of the organisational structure** as well as the observance of bank-internal policies and procedures (organisational guidelines, allocation of competences, internal guidelines etc.) and operating procedures.

(39) The expediency check in particular contains the checking of the **proportionality** of the allocation of funds and achieving of targets while taking into consideration the economy and efficiency of the organisation, procedural processes, and the allocation of resources (especially in terms of staffing and material resources).

(40) The nature, scope, frequency and methods used in audits shall be primarily guided by the **risk profile of the** respective **audit area,** and shall guarantee that the audit results provide sufficient information about the legality, propriety and expedience within the respective audit area.

B. AUDIT AREAS

(41) Internal auditing audits the following areas in a risk-based manner:

a. all the credit institution's operating areas and business lines;[13]

b. all the credit institution's operating and business processes;[14]

c. bank-internal rules and procedures (organisational guidelines, allocation of competences, guidelines etc.) and operating procedures, also with regard to their being observed up-to-date and being updated on an ongoing basis;

d. the appropriateness of policies and procedures pursuant to lit. c in light of the legal and supervisory requirements and the credit institution's risk appetite and risk strategy;

[12] Required theoretical knowledge for the Head of the Internal Audit Function is especially assumed to exist, where they can prove that they have successfully completed a relevant sectoral training, a university degree or course of studies from a university of applied sciences with a relevant specialisation, an internationally recognised training programme for internal auditors or a professional examination pursuant to Article 13 of the Cooperative Auditing Associations Act (**GenRevG**; Genossenschaftsrevisionsgesetz).

[13] The credit institution's operating areas and business lines cover for example financing, accounting, risk management or participation management.

[14] The institution's operating and business processes include for example the granting of loans, further processing of loans, loan processing control and valuation measures.

e. all legally prescribed audit areas (especially those stipulated in BWG, WAG 2018, Delegated Regulation (EU) 2017/565 and FM-GwG).

(42) Since internal auditing is legally obliged to undertake a **comprehensive audit**, **the list of audit areas shown here is demonstrative and non-exhaustive**, as other audit areas for internal auditing may also arise that are necessary for the orderly performance of the function. In particular, all outsourced areas of the credit institution should also be audited.[15]

(43) Individual audit areas should not be considered in an isolated context. Cooperation between the individual specialised staff members in internal auditing is both advisable and necessary, especially for **audits across multiple departments** (spread across multiple organisational units). The Head of the Internal Audit Function must ensure an orderly cooperation within the internal audit function.

VI. CONDUCTING OF AUDITS BY THE INTERNAL AUDIT FUNCTION

A. AUDIT PLANNING

(44) The internal audit function shall draw up an **annual audit plan** and its audit activities shall be conducted in accordance with this plan (Article 42 para. 5 BWG, cf. also IG-GL paras. 205-207). This internal audit plan must be finalised annually, at latest during the fourth quarter.

(45) The management body (in its management function) as well as the supervisory board or the supervisory body that is competent under law or the articles of association shall be explicitly be made aware of the internal audit plan. **Similarly, all executive directors will be explicitly be made aware about significant changes to the internal audit plan.** The size and nature of the credit institution to be audited, as well as the nature, scale, complexity and risk profile of its business activities, will be taken into account appropriately in the internal audit planning. The internal audit planning is to be adequately documented. The internal audit plan is to be retained for at least seven years.

(46) The internal audit plan must in particular contain the audit areas to be audited, the audit effort stated in person days and the type of audit.

(47) The underlying **frequency of audits** upon which the internal audit plan is based is **determined** as follows in the **organisational guidelines** for internal auditing (cf. Chapter IV.A. for further detail).

a. Audit areas, for which explicit orders exist regarding the frequency of audits, are required to be audited in accordance with such orders;

b. All other audit areas must be audited using a risk-based approach at appropriate intervals. Accordingly, high-risk areas must be audited more frequently; in the case of lower risk areas - such as support areas - a lower frequency may suffice.

[15] Cf. also paras. 50 et seq. EBA Guidelines on Outsourcing (EBA/GL/2019/02) regarding the internal audit functions.

(48) In addition, the internal audit function shall draw up an **audit map**, containing a detailed overview of all audit areas also stating their audit intervals pursuant to MN 47. The audit map, which is adapted to the current requirements on an ongoing basis, forms the basis for audit planning.

B. SPECIAL AUDITS

(49) The internal audit function is required to conduct **unscheduled audits on an ad hoc basis** (Article 42 para. 5 BWG).

(50) **Special audits** may be initiated at the proposal of a director, or autonomously by the internal audit unit itself. A special audit is required to be initiated when **ordered by at least two executive directors**. Furthermore, **the supervisory board or the competent supervisory body in accordance with the articles of association** may also request a special audit to be conducted.

C. WORKING PAPERS

(51) Every audit shall be **documented** by means of working papers, from which, as a minimum, it shall be possible to determine **audit activities conducted as well as their findings** in a way that remains plausible for third-party experts at all times.

(52) All audit activities and findings are to be **clearly documented by means of working papers**: Working papers corroborate the audit activities performed and the circumstances under which the findings were reached. Working papers are to be retained in paper form, electronically or in another suitable manner.

(53) Material **working papers** are to be retained for every audit conducted **for at least seven years**.

D. INFORMATION RIGHTS OF THE INTERNAL AUDIT FUNCTION

(54) The staff members of the internal audit function shall be afforded **comprehensive and unrestricted information**, **submission, inspection and audit rights**. Neither data protection law (cf. Article 6 (1) (c) of the General Data Protection Regulation ("**GDPR**") in conjunction with Article 42 BWG), nor banking secrecy requirements in accordance with Article 38 BWG, nor other comparable legal impediments under foreign jurisdictions shall be allowed to prevent this. Such rights also exist towards third parties active on behalf of the credit institution and all credit institutions within the group of credit institutions as defined in Article 30 BWG provided this is necessary to fulfil the internal audit function's remit. The rights do not relate to the activities of the works council or other bodies in relation to the workforce as defined in Article 40 of the Labour Constitution Act (ArbVG; Arbeitsverfassungsgesetz) within the scope of their activity for such a body as well as for disabled persons' representatives pursuant to Article 22a of the Disability Employment Act (BEinstG; Behinderteneinstellungsgesetz).

(55) **Instructions and resolutions by the management body and other bodies of the credit institution** that may be significant for the internal audit function shall be **made available to the Head of the Internal Audit Function without delay and without having to be requested**. The internal audit function shall

be informed about significant changes in the audit areas in a timely manner (cf. Chapter V.B for further details).

E. REPORTING OBLIGATIONS

(56) The heads of the audited organisational units shall be **explicitly informed about the findings of audits in a concluding meeting.** They will have the **opportunity to comment**.

(57) A **written internal audit report** shall be drawn up as a follow-up to every audit, which shall explicitly submitted to the heads of the audited organisational units and those persons they directly report to.

(58) The internal audit report shall at least contain the audit area and the findings of the audit (especially deficiencies identified **and the necessary and recommended measures to be taken including an appropriate deadline for their being remedied or implemented) specifically highlighting material deficiencies, threats and risks**.[16] Furthermore, the report must also state the start and end date of the audit as well as the type of audit and the methodologies applied for the individual audits. The heads of the audited organisational units are to be given the opportunity to submit statements about the identified deficiencies, as well as the necessary and recommended measures, which where possible are to be considered in the internal audit report.

(59) The **internal audit report** is addressed to the management body in its management function in the first instance (Article 42 para. 3 BWG).[17] The internal audit function must report directly to all executive directors. In the event that all executive directors do not receive every comprehensive internal auditing report, then a written summary report must be sent to all executive directors on a regular basis about the findings of all the audits conducted during the reporting period, in particular highlighting significant deficiencies, threats and risks. The management body in its management function shall define the reporting frequency in the organisational guidelines for internal auditing (see also Chapter IV.A for further detail).

(60) The internal audit function shall report directly to the **chairperson of the supervisory board on a quarterly basis** about the audit areas and **material findings** from audits on the basis of the audits conducted, or to the supervisory body of the credit institution either competent under law or the articles of association as well as the **audit committee** (Article 42 para. 3 BWG).[18]

(61) The **quarterly report by the internal audit function to the chairperson of the supervisory board** or the supervisory body otherwise competent under applicable law or the articles of association and to the **audit committee** occurs **without influence** by the management body in its management function. The management body's right to make a statement about such reports remains unaffected.

---

[16] The duration of the audit is to be documented, expressed in person days, even though this information must not necessarily be included in the internal audit report.

[17] Nevertheless it will still be more practical - especially in the case of credit institutions organised on multiple levels - to submit the internal auditing report to the head of the organisational unit that is the subject of the audit, as well as their direct superiors and to comply with the information obligations towards the management body in its management function by means of summary reports with a predetermined reporting frequency.

[18] The reporting obligation towards the supervisory body continues to exist even where there are no material audit findings; in such cases, however, a statement must at least be made ("empty report").

(62) For transparency reasons, for documentation purposes, as well as for subsequent traceability the **quarterly report** to the chairperson of the supervisory board or the competent supervisory body under law or the articles of association and to the audit committee is required be made **in written form**. The form and scope of this report may be designed in different forms in keeping with the principle of proportionality.

(63) All reports are to be retained for at least **seven years**.

(64) Irrespective of such reports, **the internal audit function shall inform** all executive directors as well as the supervisory board or the competent supervisory body under law or the articles of association **without delay** and demonstrably, where in the performance of duties it becomes aware of circumstances which it considered would significantly affect the **existence of, the ability of the credit institution to function, its performance, or endanger the observance of the credit institution's obligations towards its creditors**.

F. REACTION TO IDENTIFIED DEFICIENCIES

(65) All deficiencies identified by the internal audit function are to be remedied in the course of a formal programme for remedying deficiencies by the competent heads of the audited organisational units in a timely manner by means of actions that are suitable for remedying deficiencies. **They shall inform the internal audit function about the implementation of the necessary measures as well as the identified deficiencies having been remedied.**

(66) The internal audit function shall check that the **necessary measures are implemented in a timely fashion** and that **identified deficiencies are remedied in a timely manner**, and shall also conducts necessary follow-up audit activities.

(67) In the event that the necessary measures are not implemented in a timely manner and/or the identified deficiencies are not remedied in a timely manner without objectively justified reasons for failing to do so, the internal audit function shall the person that the heads of the audited organisational units directly report to about this without delay. Where the necessary measures continue not to be implemented or deficiencies continue not to be rectified, then the competent executive directors shall be informed about this circumstance.

VII. GROUP INTERNAL AUDIT

(68) In the case of **groups of credit institutions as defined in Article 30 BWG**, the internal audit function of the superordinate credit institution as defined in Article 30 para. 5 BWG shall perform the **tasks of group internal auditing** (Article 42 para. 7 BWG).

(69) Internal group auditing reports directly to the management body in its management function of the superordinate credit institution and audits all entities in the group of credit institutions as defined in Article 30 BWG.

(70) The tasks of Group Internal Audit shall in particular include:

a. harmonisation of internal auditing standards within the group of credit institutions;
b. reviewing the expediency of the organisational structure and procedures;
c. reviewing compliance with regulatory standards; as well as
d. reviewing legality, propriety and expedience with regard to:
   - consolidated accounting;
   - the ability to function, internal audit plans and audit reports of the internal audit function of subordinate credit institutions;
   - as well as consolidated reporting pursuant to Article 30 paras. 7, 8, 9, and 10 BWG.

(71) The group internal audit function audits all entities within the group of credit institutions as defined in Article 30 BWG. **Extending group internal audit's auditing activity to include entities consolidated under the consolidated financial statement, but which are not part of the group of credit institutions, is permissible.**

(72) It is necessary for all entities within the group of credit institutions as well as **all consolidated entities** that are not part of the group of credit institutions to make **necessary documents and information** available to the group internal audit function to permit the group internal audit function to perform its statutory duties.

VIII. COMMUNICATION BY THE SUPERVISORY AUTHORITY TO THE INTERNAL AUDIT FUNCTION

A. REGULAR COMMUNICATION

(73) Within the scope of its **regular communication** (eg. within the scope of an on-site inspection or a *Supervisory Review and Evaluation Process* ("**SREP**") in accordance with Article 69 paras. 2 and 3 BWG)**, the supervisory authority discusses the deficiencies, threats and risks to which the credit institution is exposed with the internal auditing unit**. Such a dialogue does not create any additional further reporting obligations over and above the existing legal obligations for the internal audit function. Direct communication with the internal audit function allows the supervisory authority to gain an impression about how the credit institution generally handles identified weaknesses as well as the significance attributed to the findings from audits conducted by the internal audit function.[19]

[19] Cf. also Basel Committee on Banking Supervision, The Internal Audit Function in Banks, 2012.

B. NOTIFICATIONS

(74) Credit institutions are required to notify the FMA **in writing without delay about the person responsible or the head** of the internal audit function (Article 73 para. 1 no. 11 BWG).

(75) Every credit institution, in which a **separate organisational unit** is entrusted with the internal audit function, submits a notification about its **head**. Moreover, in such cases, no notifications are required about additional persons responsible for internal auditing, since the head of the internal audit function bears overall and ultimate responsibility.

(76) Credit institutions that are not obliged to establish **a separate organisational unit pursuant to Article 42 para. 6 nos. 1 and 2 BWG**, but which are not affiliated to a central institution or are not part of a group of credit institutions, shall notify a person responsible for internal auditing.

(77) Credit institutions that under Article 42 para. 6 nos. 3 and 4 BWG may outsource their internal auditing within a group of credit institutions or a sectoral association to a separate organisational unit for internal auditing, send a notification about that unit's head.[20] A **collective notification** about the head of this organisational unit suffices where **several credit institutions within the same group or the same sectoral association have outsourced to the same organisational unit**. In this case, it is not necessary for every individual outsourcing credit institution to make separate notifications about the the same head. Furthermore, no further persons responsible are required to be notified within the group or the sectoral association, since the head of the organisational unit bears overall and ultimate responsibility. In all of the instances listed, no unresolved conflicts of interests exist in relation to the head of the organisational unit based on the fact that they bear principle or ultimate responsibility for the internal auditing of several credit institutions.

(78) The **notification about the head** must contain details about the **conditions in accordance with Article 5 para. 1 nos. 6 and 7 BWG as well as the non-existence of reasons for exclusion in accordance with Article 42 para. 2 BWG** being satisfied. With regard to the **documents to be submitted together with the notification**, we also refer to the **Annex to the Fit & Proper Circular**[21]. The notification of a **person responsible** is only required to consist of the **confirmation of non-existence of grounds for exclusion in accordance with Article 42 para. 2 BWG**.

C. APPLICATION IN ACCORDANCE WITH ARTICLE 42 PARA. 6 BWG

(79) Credit institutions, with **total assets exceeding EUR 1 billion**, but which are affiliated to a central institution or which belong to a group of credit institutions as defined in Article 30 BWG, may apply to the FMA to be allowed to be exempted from the requirement to have a separate organisational unit for the internal audit function (Article 42 para. 6 final sentence BWG), where a separate organisational unit

[20] This also applies to credit institutions, which while not obliged to establish a separate organisational unit pursuant to Article 42 para. 6 nos. 1 and 2 BWG nevertheless outsource their internal audit function within the group of credit institutions or to the sectoral association.
[21] Cf. footnote 11.

for the internal audit function exists within the group of credit institutions or within the sectoral association that is appropriately staffed, both in qualitative and quantitative terms (cf. Chapters IV.D. and IV.E.).

(80) **To reduce the number of follow-up enquiries, the FMA recommends attaching the following documents to the application:**

- The organisational chart of the credit institution, in which the organisational unit for the internal audit function is housed;
- Description of the structural and procedural organisation of the organisational unit (number of employees (full-time equivalents), reporting obligations, procedures in the event of deficiencies being determined);
- Confirmation of there being adequate audit capacities for all credit institutions that are to be audited;
- A written agreement as defined in Article 25 para. 1 BWG ("outsourcing contract");
- Confirmation of the conditions set forth in Article 5 para. 1 nos. 6 and 7 BWG being observed as well as details about reasons for exclusion in accordance with Article 42 para. 2 BWG not existing regarding the head of the internal audit function in the organisational unit, into which outsourcing occurs;
- Confirmation about reasons for exclusion in accordance with Article 42 para. 2 BWG not existing regarding the staff members of the internal audit function in the organisational unit, to which outsourcing occurs.

In addition to the application in accordance with Article 42 para. 6 BWG, no additional application in accordance with Article 25 BWG is necessary, provided all the aforementioned documentation has been attached to the application under Article 42 para. 6 BWG.