Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circular 2017/1
Corporate governance – banks

Corporate governance, risk management and internal controls at banks

Reference:	FINMA Circ. 17/1 "Corporate governance – banks"
Date:	22 September 2016
Entry into force:	1 July 2017
Concordance:	former FINMA Circ. 08/24 "Monitoring and internal control - banks", dated 20 November 2008
Legal framework:	FINMASA Article 7 para. 1 let. b
	BA Articles 3 para. 2 lets. a and c, 3*b*–3*f*, 4^{quinquies} and 6
	BO Articles 11 para. 2 and 12
	SESTA Articles 10 para. 2 let. a and para. 5 and Article 14
	SESTO Articles 19 and 20
	CAO Articles 7–12

Addressees																																
BankA			ISA			SESTA	FMIA							CISA										AMLA			Other					
Banks	Financial groups and congl.	Other intermediaries	Insurers	Insurance groups and congl.	Intermediaries	Securities dealers	Trading venue	Central counterparties	Central securities depositories	Trade repositories	Payment systems	Participants	Fund management companies	SICAVs	Limited partnerships for CISs	SICAFs	Custodian banks	Asset manager CISs	Distributors	Representatives of foreign CISs	Other intermediaries	SROs	DSFIs	SRO-supervised institutions	Audit firms	Rating agencies						
X	X					X																										

Laupenstrasse 27, 3003 Bern
Tel. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
www.finma.ch

Index

I.	**Subject matter**	Margin no.	1
II.	**Terms**	Margin no.	2-7
III.	**Scope of application (the principle of proportionality)**	Margin no.	8
IV.	**Board of directors**	Margin no.	9-46
A.	Duties and responsibilities	Margin no.	9-15
B.	Members of top management	Margin no.	16-25
C.	Basic principles governing a directorship	Margin no.	26-29
D.	Committees and the division of responsibilities	Margin no.	30-46
V.	**Executive board**	Margin no.	47-51
A.	Duties and responsibilities	Margin no.	47-50
B.	Requirements to be met by members of the executive board	Margin no.	51
VI.	**Institution-wide risk management framework**	Margin no.	52-59
VII.	**Internal control system**	Margin no.	60-81
A.	Revenue-generating units	Margin no.	61
B.	Independent control bodies	Margin no.	62-81
VIII.	**Internal audit**	Margin no.	82-97
A.	Establishment	Margin no.	82-86
B.	Supervision and organisation	Margin no.	87-90
C.	Duties and responsibilities	Margin no.	91-97
IX.	**Group structures**	Margin no.	98-99
X.	**Transitional provisions**	Margin no.	100-105

I. Subject matter

This circular sets out the requirements to be met by the corporate governance, risk management, internal control system and internal audit at banks, securities dealers, financial groups (Art. 3*c* para. 1 BA) and financial conglomerates dominated by banking or securities trading (Art. 3*c* para. 2 BA). These are referred to below as "institutions". 1

II. Terms

Corporate governance is understood to mean the principles and structures on the basis of which an institution is directed and controlled by its governing bodies. 2

Risk management comprises the methods, processes and organisational structures used to define risk strategies and risk management measures in addition to the identification, analysis, assessment, management, monitoring and reporting of risks. 3

Risk tolerance comprises quantitative and qualitative considerations regarding the key risks which an institution is prepared to take to achieve its strategic business objectives in the context of its capital and liquidity planning. Where relevant, risk tolerance is defined per risk category as well as per institution. 4

The risk profile provides an overall picture of the risk positions entered into by an institution at institution level and per risk category at a particular point in time. 5

The internal control system (ICS) comprises the totality of the control structures and processes which at all levels of an institution form the basis for achieving its business objectives and ensuring orderly business operations. The ICS comprises retrospective controls and planning and management elements. An effective ICS consists of control activities which are integrated into work processes, appropriate risk management and compliance processes, and monitoring bodies – particularly an independent risk control and compliance function – which adequately reflect the size, complexity and risk profile of an institution. 6

Compliance is understood to mean abiding by the relevant statutory, regulatory and internal rules and observing generally accepted market standards and codes of conduct. 7

III. Scope of application (the principle of proportionality)

This circular applies to all institutions as defined in margin no. 1. The requirements are to be implemented on a case-by-case basis, giving due consideration to the size, complexity, structure and risk profile of each institution. FINMA can relax or tighten the rules in individual cases. 8

IV. Board of directors

A. Duties and responsibilities

The duties of an institution's board of directors, i.e. the governing body for guidance, supervision and control, comprise in particular: 9

a) Business strategy and risk policy

The board of directors sets out the business strategy and defines guiding principles for the institution's corporate culture. It signs off the institution-wide risk management framework and is responsible for issuing regulations, establishing and monitoring an effective risk management function, and managing overall risks. 10

b) Organisation

The board of directors is responsible for establishing an appropriate business organisation and issues the rules and regulations required to achieve this. 11

c) Finances

The board of directors bears ultimate responsibility for the financial situation and development of the institution. It approves/signs off the capital and liquidity plans, the annual report, the annual budget, the interim financial statements and the financial objectives for the year. 12

d) Personnel and other resources

The board of directors is responsible for ensuring that an institution has appropriate levels of personnel and other resources (e.g. infrastructure, IT) and for the personnel and remuneration policies. It appoints and dismisses the members of its committees, the members of the executive board, the chair of the executive board, the chief risk officer (CRO) and the head of internal audit.[1] 13

e) Monitoring and control

The board of directors oversees the work of the executive board. It is responsible for ensuring that there is both an appropriate risk and control environment within the institution and an effective ICS. It appoints and monitors the internal audit, commissions the regulatory audit firm and assesses its reports. 14

[1] The head of internal audit can also be selected by the audit committee.

f) Major structural changes and investments

The board of directors takes decisions on major changes to the company and group structure, major changes in significant subsidiaries, and other strategically important projects. 15

B. Members of the board of directors

a) General prerequisites

The board of directors in its totality has adequate management expertise and the prerequisite specialist knowledge and experience of the banking and financial services sector. It is diversified to the extent that all key aspects of the business, including finance, accounting and risk management, are adequately represented. 16

b) Independence

At least one third of the board of directors consists of independent members. FINMA may approve exceptions (e.g. for domestic financial groups) where there is good reason for doing so. 17

Members of the board of directors are deemed to be independent if they: 18

- are not and have not in the previous two years been employed in some other function within the institution; 19
- have not been employed in the previous two years by the institution's audit firm as lead auditor (of the regulatory audit) responsible for the institution; 20
- have no commercial links with the institution which, in view of their nature and scope, would lead to conflicts of interest; and 21
- are not a qualified participant (within the meaning of Art. 3 para. 2 let. c^{bis} BA and Art. 10 para. 2 let. d SESTA) of the institution and represent no such participant. 22

Members of the board of directors of cantonal or communal banks who have been appointed or selected by cantons, municipalities or other cantonal or communal institutions governed by public law are deemed to be independent within the meaning of margin no. 18 ff. provided that they: 23

- do not belong to the cantonal or communal government or administration or another cantonal or communal body governed by public law, and 24
- have received no instructions from their appointing body regarding their activity as members of the board of directors. 25

C. Basic principles governing a directorship

All members of the board of directors devote sufficient time to their roles and play an active part in strategic corporate governance. Members must perform their function in person and be permanently prepared to intervene in crisis situations and emergencies besides the normal pattern of meetings. 26

The board of directors defines the requirements profile for its members, its chair, any members of committees, and the chair of the executive board. It approves and periodically assesses the requirements profile for the other members of the executive board, as well as for the CRO and the head of internal audit. It is responsible for succession planning. 27

At least once a year the board of directors, where necessary with the assistance of a third party, critically assesses its own performance (meeting of targets and method of operating) and records the results in writing. 28

The board of directors defines how conflicts of interest are to be handled. All current and previous conflicting interests must be disclosed. If a conflict of interest cannot be avoided, the institution takes appropriate steps to ensure that it is effectively limited or removed. 29

D. Committees and the division of responsibilities

a) Role of the chair

The chair presides over the board of directors as a whole and represents it internally and externally. That person has a key role in shaping the strategy, communications and culture of the company. 30

b) Committees

Institutions in supervisory categories 1 to 3 must establish an audit committee and a risk committee. Institutions in supervisory category 3 may combine these into a single committee. Systemically important institutions must establish, at least at group level, a compensation and nomination committee. The committees are responsible for ensuring appropriate reporting to the board of directors. 31

The personnel composition of the audit committee must differ sufficiently from that of other committees. 32

A majority of the members of the audit and risk committees must be substantially independent (see margin no. 18 ff.). As a matter of principle, the chair of the board of directors must be neither a member of the audit committee nor chair of the risk committee. Each committee as a whole must have sufficient knowledge and experience of the areas for which it is responsible. 33

c) Responsibilities of the audit committee

These include in particular: 34

- drafting general guidelines for internal auditing and financial reporting for submission to the board of directors; 35
- monitoring and assessing the financial reporting and the integrity of the financial statements, including discussion of these topics with the member of the executive board who is responsible for finance and accounting, the lead auditor of the financial audit, and the head of internal audit; 36
- monitoring and assessing the effectiveness of the internal control system, specifically risk control, the compliance function and internal audit (in so far as this responsibility is not discharged by the risk committee); 37
- monitoring and assessing the effectiveness and independence of the regulatory audit firm and its interaction with internal audit, including discussion of the audit reports with the lead auditor; 38
- assessing the regulatory audit plan, audit rhythm and audit results produced by the internal audit and the regulatory audit firm. 39

d) Responsibilities of the risk committee

These include in particular: 40

- discussing the institution-wide risk management framework and presenting relevant recommendations to the board of directors; 41
- assessing the institution's capital and liquidity planning and reporting to the board of directors; 42
- assessing, at least annually, the institution-wide risk management framework and ensuring that necessary changes are made; 43
- controlling whether the institution has adequate risk management with effective processes which are appropriate to the institution's particular risk situation; 44
- monitoring the implementation of risk strategies, ensuring in particular that they are in line with the defined risk tolerance and risk limits defined in the institution-wide risk management framework. 45

The risk committee receives regular reports from the CRO and other relevant office holders on the respective aspects of the institution-wide risk management framework (see margin 46

no. 52 ff.) and compliance with it.

V. Executive board

A. Duties and responsibilities

The executive board is responsible for operational business activities which reflect the business strategy and the targets and resolutions of the board of directors and is also responsible in particular for: 47

- managing day-to-day business, operational revenue and risk management, including management of the balance sheet structure and liquidity and representing the institution vis-à-vis third parties in operational matters; 48

- submitting applications regarding transactions for which the board of directors is responsible or for which its approval is required, and issuing rules for regulating business operations; 49

- developing and maintaining effective internal processes, an appropriate management information system (MIS), an ICS and the necessary technological infrastructure; 50

B. Requirements to be met by members of the executive board

Members of the executive board, both individually and as an overall body, must have adequate management expertise and the specialist knowledge and experience of banking and financial services required to ensure compliance with licensing requirements in the context of the institution's operational activities. 51

VI. Institution-wide risk management framework

The institution-wide risk management framework is developed by the executive board and approved by the board of directors. 52

The framework comprises the risk policy and risk tolerance and the risk limits based on them in all key risk categories. 53

The framework must take account of the following aspects: 54

- standardised categorisation[2] of key risks to ensure consistency with risk management objectives; 55

- specification of potential losses from these key risk categories; 56

[2] By class, type and level and in line with the definitions set out in the Capital Adequacy Ordinance (CAO).

- definition and application of the tools and organisational structures required to identify, analyse, evaluate, manage and monitor the key risk categories and for reporting purposes; 57

- development of documentation which enables appropriate verification of the definition of risk tolerance and the corresponding risk limits; 58

- provisions relating to risk data aggregation and reporting for institutions in supervisory categories 1 to 3. In the case of systemically important institutions, these provisions must include information about data architecture and IT infrastructure which enables an aggregated and timely risk analysis/assessment and risk data aggregation/reporting across all of the institution's key risk categories both under normal circumstances and in periods of stress. 59

VII. Internal control system

There are at least two controlling bodies within the ICS: the revenue-generating units, and the control bodies which are independent of them. 60

A. Revenue-generating units

Revenue-generating units carry out their control function as part of everyday business activities by managing risks and specifically by directly monitoring, managing and reporting on them. 61

B. Independent control bodies

The independent control bodies monitor risks and compliance with statutory, regulatory and internal rules. Individual institutions can establish a variety of control bodies which must, however, at least cover the duties and responsibilities of risk control (margin no. 69–76) and the compliance function (margin nos. 77–81). 62

The compensation system for independent control bodies must not create incentives which could lead to conflicts of interest with the duties of these bodies. 63

a) Establishment and supervision

In the context of their duties, the independent control bodies have unlimited information, access and inspection rights and are to be integrated independently from the revenue-generating units into the overall organisation or the ICS. They must be provided with the necessary resources and powers. 64

The institution defines one or more persons on the executive board to be responsible for the independent control bodies. 65

It ensures that the independent control bodies have direct access to the board of directors. 66

Institutions in supervisory categories 1 to 3 have an autonomous risk control and compliance function as independent control bodies. They appoint a CRO who, in addition to risk control, can also be responsible for other independent control bodies. 67

Systemically important institutions appoint a CRO who is a member of the executive board. 68

b) Duties and responsibilities of risk control

Risk control ensures comprehensive and systematic monitoring of and reporting on individual and aggregated risk positions. This includes conducting stress tests and scenario analysis under unfavourable operating conditions as part of the quantitative and qualitative analysis. 69

In the case of institutions in supervisory categories 1 to 3, risk control also ensures the appropriate implementation of provisions relating to risk data aggregation and reporting as set out in margin no. 59. 70

Risk control also monitors the institution's risk profile in line with the risk tolerance and risk limits defined in the institution-wide risk management framework. 71

Risk control is also responsible for developing and operating adequate risk monitoring systems, defining and applying principles and methods for risk analysis and assessment (e.g. assessment and aggregation methods, validation of models), and monitoring systems to ensure compliance with supervisory regulations (especially regulations relating to capital adequacy, risk diversification and liquidity). 72

Risk control is to be appropriately consulted during the development of new or expanded product categories, services or business/market areas and for major or complex transactions. 73

Risk control is actively involved in the process of defining risk limits and ensures that risk limits are consistent with the defined risk tolerance and reconciled to the results of the stress tests and that they are defined in such a way as to constitute an operationally effective management tool for the executive board. 74

Risk control reports to the executive board at least every six months and to the board of directors at least annually on the institution's risk profile and its activities as defined in margin no. 69 ff. A copy of these reports must be provided to internal audit and the regulatory audit firm. 75

In the event of special developments, risk control promptly informs the executive board and internal audit. If matters with far-reaching implications are involved, it also informs the board of directors. 76

c) Duties and responsibilities of the compliance function

The duties and responsibilities of the compliance function include at least the following activities: 77

- conducting an annual assessment of the compliance risk of the institution's business activities and developing a risk-oriented activity plan for approval by the executive board. The activity plan must also be made available to internal audit; 78
- reporting promptly to the executive board on any major changes in the compliance risk assessment; 79
- reporting annually to the board of directors on the assessment of compliance risk and the activities of the compliance function. A copy of the relevant reports must be provided to internal audit and the regulatory audit firm; 80
- reporting serious compliance breaches and matters with far-reaching implications in a timely manner to the executive board and the board of directors, as well as supporting the executive board in its choice of appropriate instructions and measures. Internal audit must be informed accordingly. 81

VIII. Internal audit

A. Establishment

Every institution shall establish an internal audit function. 82

If it seems inappropriate to establish an internal audit, the relevant duties and responsibilities can be delegated to: 83

- internal audit of the parent company or to the internal audit of another group company, provided that this is a bank, a securities dealer or another officially supervised financial intermediary (e.g. an insurance company) (for foreign banks see Art. 4^{quinquies} BA), 84
- a second audit firm which is independent of the institution's regulatory audit firm, or 85
- a group company or independent third party, provided that the regulatory audit firm confirms that it has the necessary expertise and appropriate technical and personnel resources. 86

B. Supervision and organisation

Internal audit reports to the board of directors or its audit committee and fulfils the auditing and monitoring responsibilities assigned to it in an independent fashion. It has an unlimited right of inspection, information and audit within the institution and its consolidated compa- 87

nies as defined in margin no. 98.

Internal audit must adequately reflect the size, complexity and risk profile of the institution and forms an organisationally autonomous unit which is independent of business operations. 88

Internal audit must meet the qualitative requirements defined by the Institute of Internal Auditing Switzerland (IIAS). The work of internal audit is based on the International Standards for the Professional Practice of Internal Auditing, as issued by the Institute of Internal Auditors (IIA). 89

The compensation system for employees of internal audit must not define incentives which could lead to conflicts of interest. 90

C. Duties and responsibilities

Internal audit delivers independent audits and assessments of the appropriateness and effectiveness of the company's organisation and business processes, particularly as regards the institution's ICS and risk management. 91

It conducts a comprehensive risk assessment of the institution on an annual basis; this takes appropriate account of external developments (e.g. the economic environment, regulatory changes) and internal factors (e.g. major projects, business strategy). 92

Based on this risk assessment and other auditing requirements, internal audit defines the audit objectives and planning for the next audit period and submits them and any necessary changes to the board of directors or its audit committee for approval. 93

Internal audit ensures that the executive board and the regulatory audit firm are informed about the risk assessment and audit objectives. 94

Internal audit reports in writing in a timely manner on all material findings both to the board of directors or its audit committee and to the executive board. 95

Internal audit publishes a report setting out the key audit findings and important activities in the audit period at least annually and submits this report with any corresponding conclusions to the board of directors or its audit committee, the executive board and the regulatory audit firm for their information. 96

Furthermore, internal audit or another independent unit within the institution (e.g. the compliance function or risk control) informs the board of directors or its audit committee at least every six months about progress made in eliminating major shortcomings and/or implementing the recommendations of internal audit or the regulatory audit firm. 97

IX. Group structures

This circular applies by extension to financial groups and conglomerates ("groups"). 98

Groups must regulate the duties and responsibilities of the units with overall responsibility for group management. While giving due consideration to the business activities and material risks at group and individual institution level, the defined standards must ensure the efficient and consistent management of the group, permit necessary information exchange, take account of legal and organisational structures and define the duties, responsibilities and necessary independence of the respective management levels. Particular attention must be paid to risks which arise specifically from combining a number of companies into a single business entity. 99

X. Transitional provisions

The following requirements must be implemented within one year of the circular entering into force: 100

- implementation of the one third rule on the independence of the board of directors, as set out in margin no. 17; 101
- the establishment of an audit committee and a separate risk committee for institutions in supervisory categories 1 to 3, as set out in margin no. 31; 102
- the drafting and approval of a framework for institution-wide risk management, as set out in margin no. 52 ff.; 103
- the maintenance of a separate CRO position, also as part of the executive board for systemically important institutions, as set out in margin nos. 67 and 68; 104

The relevant later date applies to meeting the more far-reaching provisions on risk data aggregation and reporting, as set out in margin no. 59 for systemically important banks: 105

- entry into force of this circular, and
- a three-year transitional period following designation as a systemically important bank within the meaning of Article 8 para. 3 BA.