Circular 06/6 of the Swiss Federal Banking Commission Supervision and Internal Control

Unofficial translation
by PricewaterhouseCoopers

February 2007

PricewaterhouseCoopers

Circular 06/6 of the Swiss Federal Banking Commission Supervision and Internal Control dated 27 September 2006

Table of Contents

Unofficial translation by PricewaterhouseCoopers

I. Object

This circular sets guidelines for corporate governance, the supervision of business activities and internal control, and the supervision thereof by the responsible function in banks, securities dealers, financial groups (Art. 3c para. 1 BA) and financial conglomerates mainly engaged in banking and securities dealing (Art. 3c para. 2 BA). Henceforth, these will be referred to as institutions[1]. 1

Internal control (synonymous with the internal control system) encompasses all controlling structures and processes which allow a company to reach its business policy targets on all levels, and support the orderly operation of the institution. Internal control not only encompasses retroactive controlling activities but also includes those with a planning and steering aspect. Inter alia, an effective internal control entails control activities which are integrated in business processes, processes for risk management and adherence to applicable standards (compliance), a risk control independent of risk management, as well as a compliance function. Internal audit audits and assesses the internal controls and thereby ensures continuous improvement. 2

II. Scope

The circular is applicable to institutions described in margin no. 1, with the following exceptions: 3

- Securities dealers without bank status: if these do not have a segregation of duties between board of directors and management, margin nos. 18–40 are not applicable. However, margin nos. 41–53 apply analogously. 4
- Private bankers: margin nos. 18–40 are not applicable. However, margin nos. 41–53 apply analogously. Of the remaining provisions, deviations and simplifications are possible as long as the partners are personally liable and responsible for business management. Additionally, the auditor and regulatory authorities must be consulted for these to be applicable. 5
- Directly or indirectly held subsidiary banks and securities dealers, as well as subsidiary companies involved in financial activities of domestic and international financial groups and financial conglomerates chiefly engaged in banking and securities trading: margin nos. 18–40 are not applicable. Nevertheless, it is recommended that such entities establish an audit committee. However, margin nos. 41–53 are analogously applicable. 6
- Branch offices of foreign institutions: margin nos. 9–53 are not applicable. All other provisions apply by analogy. 7
- The circular does not apply to companies not mainly involved in finance belonging to financial groups or conglomerates dominated by entities mainly involved in banking and securities trading. In the case of doubts, certain group companies may, upon request by the parent company, be explicitly exempted from having to adhere to the circular. 8

[1] Comment PwC: Term as used in the official English translation of SFBC circular 05/*1 Audit*

III. Board of Directors

A. Duties and Responsibilities

a) Supervision and internal control

The board of directors, e.g. the body for the guidance, supervision and control, carries the responsibility for the regulation, establishment, continuity and regular supervision of an internal control function adequate in relation to the size, the complexity, the structure and risk profile of the institution. 9

By establishing an internal control function based on a systematic risk analysis and its supervision of such, the board of directors ensures that all of the institution's material risks are recorded, mitigated and supervised. With financial groups and financial conglomerates dominated by entities active in banking and securities trading, it is especially important to consider the risks which may arise from the combination of several companies to a single economic entity. The systematic risk analysis must be documented in writing. 10

The board of directors regularly discusses with management its assessment of the adequacy and effectiveness of the internal controls. 11

b) Control environment

By issuing guidelines for management, the board of directors ensures that all employees on all levels are aware of and understand their responsibilities and tasks in regard to the internal control processes. 12

The board of directors ensures that no employee at any level succumbs to the pressure to attain goals by circumventing the mechanisms of control. It ensures that the system of remuneration does not offer any incentive to disregard the mechanisms of control. 13

The board of directors ensures that there are rules for handling conflicts of interests. If a conflict of interest cannot be avoided, the institution takes measures to properly deal with the conflict of interest. 14

c) Implementing and supervising an internal audit function

The board of directors establishes an internal audit function which directly reports to the audit committee (or another committee). Please refer to margin nos. 54–79 for further information on its organisation, tasks and responsibilities, as well as its accountability and its duty to report. 15

The board of directors or the relevant committee supervises and assesses the internal audit department, and periodically makes sure that it has adequate resources and authorities, as well as the necessary independence and objectivity in order to assume its auditing responsibilities for the institution. 16

B. Members of the Board of Directors

a) General requirements

In order to properly execute its tasks, the board of directors, as a body, must comply with the requirements, (especially technical expertise, experience, and availability) and assess its own achievement of goals and working style at least annually, documenting this in writing. 17

b) Independence

The members of the board of directors structure their personal and business relations so as to avoid possible conflicts of interest with the institution. According to Art. 8 para. 2 BO, a member of the board is prohibited from holding a managerial function in the institution. 18

At least one third of the board of directors should consist of members that fulfil the criteria of independence stipulated in margin nos. 20–24. These members are to be named in the annual report. If fewer than a third of the members fulfil the criteria of independence, the reason for this must be given in the annual report[2]. 19

A member of the board of directors is considered independent if he/she at least fulfils the following criteria. He/she 20

- is not active in any other function in the institution or has not been active there in the last two years; 21
- has not been employed as the lead auditor responsible for this institution at the institution's audit firm in the last two years; 22
- may not have any business relations with the institution which, because of their type or scope, may lead to a conflict of interest, and 23
- is neither a qualified participant (according to Art. 3 para. 2 lit. c^{bis} BA and Art. 10 para. 2 lit. d SESTA) of the institution nor represents such. 24

Members deployed or elected to the board of directors of a cantonal or communal bank by cantons, communities or other cantonal or communal public institutions are considered independent according to margin no. 24 if they: 25

- are not part of the cantonal or communal government or administration or belong to any other cantonal or communal public body, and 26
- do not receive any instructions in regard to their activity in the board of directors from their elective body. 27

C. Segregation of Duties between Board of Directors and its Committees

The board of directors may establish committees or allocate certain tasks to individual members for its support. 28

From a certain size or complexity of the institution onwards, the board of directors must set up an audit committee (see margin nos. 32–36). 29

Should an institution not have an audit committee, the board of directors appoints one or two independent members of the board who fulfil the requirements stipulated in margin nos. 39 (however not the chairman of the board), with the duties stipulated in margin nos. 41–53. The regulatory authority may grant exceptions. If the chairman of the board is appointed to the above-mentioned function, the reason for this must be given in the annual report. 30

Tasks and authorities delegated to committees and individuals, as well as the related duties to inform, vote and report, are to be outlined by the board of directors. In all cases, the responsibility for these assigned tasks remains with the board of directors as a whole. 31

[2] Comment PwC: in the sense of Art. 6 para. 1 BA

D. Audit Committee

a) Criteria for implementing an audit committee

Institutions must establish an audit committee if at least one of the criteria specified in margin nos. 33–36 apply: 32

- balance sheet total > CHF 5 billion 33
- safe-custody volume (clients' securities and precious metals, with the exception of the banks, according to regulatory reporting AU 001/AU 101) > CHF 10 billion 34
- required capital resources according to capital resources ordinance (CRO) > CHF 200 million 35
- listed on a stock exchange (equity interest) 36

If, despite the applicability of one or several criteria stipulated in margin nos. 33–36, an institution does not establish an audit committee, the reasons must be given in its annual report. 37

b) Requirements for the members of the audit committee

The majority of the members must fulfil the requirements of independence stated in margin nos. 20–24; if less than the majority fulfils these requirements, the reason for this must be given in the annual report. 38

Members of the audit committee have sound expertise and experience in finance and accounting, and are familiar with the activities of the internal and the external auditors. 39

The chairman of the board should not be part of the audit committee. If the institution decides that he/she should be part of the audit committee, it must explain this decision in its annual report. 40

c) Tasks of an audit committee

The audit committee may delegate tasks within the range of its duties. 41

aa) Supervision and assessment of the integrity of the financial statements

The audit committee:

- critically analyses the financial statements, i.e. the stand-alone and, if necessary, consolidated financial statements, the financial statements and published interim results, as well preparation of such according to the applicable accounting principles, and in particular assesses the valuation of material balance sheet and off-balance sheet items; 42
- discusses financial statements and the quality of the underlying accounting processes with the member of Management responsible for finance and accounting, with the lead bank auditor and with the head of internal audit; 43
- informs the board of directors of all tasks it has performed according to margin nos. 42–43 and makes a recommendation as to whether the financial statements should be submitted to the shareholders' general meeting. All members of the board of directors must decide on this. 44

b) Requirements for the members of the audit committee

The majority of the members must fulfil the requirements of independence stated in margin nos. 20–24; if less than the majority fulfils these requirements, the reason for this must be given in the annual report. **38**

Members of the audit committee have sound expertise and experience in finance and accounting, and are familiar with the activities of the internal and the external auditors. **39**

The chairman of the board should not be part of the audit committee. If the institution decides that he/she should be part of the audit committee, it must explain this decision in its annual report. **40**

c) Tasks of an audit committee

The audit committee may delegate tasks within the range of its duties. **41**

aa) Supervision and assessment of the integrity of the financial statements

The audit committee:

- critically analyses the financial statements, i.e. the stand-alone and, if necessary, consolidated financial statements, the financial statements and published interim results, as well as preparation of such according to the applicable accounting principles, and in particular assesses the valuation of material balance sheet and off-balance sheet items; **42**
- discusses financial statements and the quality of the underlying accounting processes with the member of Management responsible for finance and accounting, with the lead bank auditor and with the head of internal audit; **43**
- informs the board of directors of all tasks it has performed according to margin nos. 42–43 and makes a recommendation as to whether the financial statements should be submitted to the shareholders' general meeting. All members of the board of directors must decide on this. **44**

bb) Supervision and assessment of the internal control function in regard to financial reporting

The audit committee:

- supervises and assesses whether the internal control related to the financial reporting is adequate and effective; **45**
- ensures that the internal controls for financial reporting are adjusted to reflect any major changes in the risk profile of an institution. **46**

cc) Supervising and assessing the effectiveness of the audit firm and co-operation with internal audit

The audit committee:

- appraises the risk analysis, the audit strategy based on this and, accordingly, the risk-oriented audit plan submitted by the audit firm (SFBC circular 05/1 Audit, Annex 1) once a year, or whenever there have been any major changes in the institution's risk profile; **47**
- critically analyses the audit reports on the financial and the regulatory audits (see SFBC circular 05/2 Audit Report) and discusses these with the lead bank auditor; **48**
- ascertains that shortcomings have been remedied or that recommendations of the audit firm have been implemented; **49**
- assesses the audit firm's performance and fees and ascertains its independence; **50**
- assesses the co-operation between audit firm and internal audit. **51**

dd) Assessing the internal control and internal audit of areas beyond financial reporting

The audit committee:

- assesses the effectiveness of internal controls that go beyond the area of financial reporting, namely the compliance function and risk controlling, as far as this is not already performed by other board committees; **52**
- must be informed on the audit results of internal audit and be in regular contact with its head, even if, according to margin nos. 28 and 31, internal audit is subordinated to the full board of directors or another board committee. **53**

IV. Internal Audit Function

A. Implementation

Institutions must set up an internal audit function (see Art. 9 para. 4 BO and Art. 20 para. 2 SESTO). **54**

In specific cases, the regulatory authority may, after consulting with the audit firm, exempt an institution of the duty specified in margin no. 54. **55**

Should the establishment of an internal audit function be considered inappropriate, such internal auditing duties may be delegated as follows: **56**

- to internal audit of the parent company or of another group company, as long as this is also a bank, a securities dealer or another entity (e.g. insurance company) subject to regulatory supervision by a state (for foreign banks, this applies in the framework of Art. $4^{\text{quinquies}}$ BA). **57**
- to a second audit firm, which is independent of the institution's audit firm, or **58**
- to an independent third party, provided the audit firm has confirmed the third party's professional capabilities. **59**

B. Subordination and Organisation

Internal audit reports directly to the board of directors or one of its committees and performs the auditing and supervisory tasks it is assigned. Internal audit reports mainly to the board committee to which it is directly subordinated. **60**

The internal audit department of a financial group or financial conglomerate minimally covers all companies that are subject to consolidation according to Art. 13b–g BA, Art. 10, para. 5, and 14 SESTA and Art. 6–10 Capital Ordinance. If group companies have their own internal audit departments, functionally, these are to be subordinated to the internal audit department of the financial group or financial conglomerate. **61**

The head of internal audit is appointed by the board of directors. **62**

Internal audit works independently from daily operations. **63**

According to margin no. 61, internal audit has unlimited auditing authorities within the institution and all of the companies subject to consolidation. It has unrestricted access to all books, documents, minutes and other records, as well as data carriers and systems. All information must be provided that will assist the performance of the audit procedures. **64**

Either the board of directors or the responsible committee must enact the necessary basic principles, such as regulations detailing the organisation, tasks and responsibilities, according to the direct subordination relations. In addition, internal audit determines its own working approach (e.g. methodology, types of audit, training and continuing education). **65**

Internal audit must meet the quality standards promulgated by the Swiss Institute of Internal Auditing (SIIA). Exceptions must be explained in the annual report. Internal audit applies the Standards for the Professional Practice of the Institute of Internal Auditors (IIA). **66**

Internal audit must be appropriate to the size, the complexity and the risk profile of the institution; from an organisational point of view, it is considered an independent unit. It must be provided sufficient human resources with appropriate technical expertise and tools (e.g. IT equipment) in order to fulfil their mandate. Management must have in-depth knowledge of the institution's activities. Overall, it must be ensured that the adequacy and the appropriateness of both Management and the internal controls are assessed by qualified auditors. **67**

The remuneration system for employees of internal audit may not contain any incentives which could lead to a conflict of interests. Specifically, remunerations (e.g. salaries, bonuses, fees and premiums) may not be dependent on the performance of individual products and transactions. **68**

C. Duties and Responsibilities

a) Risk assessment, audit planning and reporting

Internal audit provides important documentation/information that serves as a basis for assessing whether the institution has an effective internal control system that is appropriate for its risk profile. **69**

Internal audit conducts a complete risk assessment of the institution at least once a year, whereas external developments (e.g. economic environment, regulatory changes) and internal factors (e.g. material projects, a new business focus) must be given sufficient consideration. **70**

Based on this risk assessment, internal audit determines the areas of audit focus and goals for the next audit period. **71**

Furthermore, internal audit ensures that all risk-relevant business activities are part of a multi-year plan, and subject to an audit either by itself or by the audit firm. **72**

Internal audit informs the board of directors or the relevant committee and management of its risk assessment and audit objectives in writing, and has the audit objectives and the audit plan approved by the board of directors or the relevant committee. It sends the audit firm a copy of its documentation. **73**

During the audit period, internal audit assesses whether there have been any material changes in the risk profile and whether the audit plan requires adapting. If the yearly planning requires major changes, these are submitted to the board of directors or the relevant committee in a timely manner for approval. It informs the audit firm of any such changes. **74**

Internal audit informs the board of directors or the responsible committee and management of all important findings in writing in a timely manner. **75**

Internal audit prepares a written report at least once a year which contains the major audit findings and the major activities during the audit period; it submits this report and the relevant conclusions to the board of directors or the responsible committee. This report must also be sent to management and the audit firm. **76**

Furthermore, it informs the board of directors or the responsible committee at least every half year of the elimination of shortcomings identified or the status of the remediation of recommendations made by internal audit or the audit firm. This information and the relevant audit tracking may also be performed by another independent body at the institution, e.g., compliance or risk control. **77**

b) Differentiation from the audit firm

Internal audit and the audit firm are to coordinate their audit activities. They co-ordinate the determined audit objectives and strategies. Each represents its own point of view and based on this, they determine a common procedure. Internal audit remains responsible for the fulfilment of its audit objectives. **78**

Internal audit submits its audit reports to the audit firm in a timely manner. The audit firm has the right to access all of internal audit's working papers. In return, the audit firm makes available its audit reports to internal audit. **79**

V. Management

A. Duties and Responsibilities

Management implements the board of directors' guidelines regarding the establishment, the maintenance and the regular testing of the internal control function. **80**

Management:

- develops appropriate processes to identify, measure, evaluate, assess and control the institution's risks This specifically encompasses the elaboration of the control activities (margin nos. 87–96) integrated in the work processes, of the compliance function (margin nos. 100–112) and of risk control (margin nos. 113–125); **81**
- maintains an organisational structure which explicitly defines responsibilities, authorities, accountability, discretionary decision-making powers, as well as information flows, and documents these; **82**
- ensures that all relevant day-to-day business is recorded, transmitted and processed (management information system); **83**
- regularly reviews the adequacy of internal controls; **84**
- periodically reports to the board of directors on the effectiveness of the internal controls and immediately informs the board of directors and internal audit in the case of material findings. **85**

B. Segregation of Duties and Control Activities

Management ensures an appropriate segregation of duties and avoids assigning responsibilities which could lead to conflicts of interest. Should a complete segregation of duties be impossible due to the size of the company, it will enforce a more entrenched sense of management responsibility among line managers. **86**

Controlling activities are to be an integral part of all work processes, e.g.: **87**

- process controls: these ensure the timely identification of deviations from targets, facilitating swift remedial action; **88**
- controls of results: the actual results are compared with the goals set. They are used if immediate corrections are not required and/or not possible; **89**
- review of conduct: this allows reviewing the conduct of individuals and organisational units. They are especially employed if no quantitative results can be observed. **90**

Control activities to be used are, among others: 91

- activity controls: the different levels of management should regularly receive and scrutinise reports on economic performance, and risk and control situations appropriate to their level of authority; 92
- physical controls: For instance, this could take place in the form of the four-eyes principle, by technically restricting access to cash and valuables, or by periodic inventories; 93
- review of adherence to specified limits; 94
- review of adherence to the system of authorities, especially reviewing authorisations related to access and changes to IT systems and master data ("golden key holders"); 95
- reviews and reconciliations, e.g. of transactions and accounting items. 96

C. Compliance (Adherence to Standards)

Compliance is considered the adherence to legal, regulatory and internal regulations, as well as the observance of the common standards and rules of professional conduct. 97

A compliance risk constitutes the risk that a regulation, standards or rules of professional conduct may be violated resulting in legal and regulatory sanctions, financial losses or damage to one's reputation. 98

Management is responsible for implementing of adequate internal systems and processes to guarantee compliance throughout the institution. It takes the necessary operational measures and precautions to ensure compliance, thereby specifically taking care to implement an effective system of directives and arranging for the integration of employees according to their level of authority. In particular for internationally active institutions, directives with cross-border effects must be guaranteed to be compatible with local legislation. 99

D. Compliance Function

a) Implementation and subordination

Each institution maintains a compliance function which has unrestricted access to information, locations and documents with the scope of its function; it must be independent from profit-generating business activities and incorporated into the overall organisation. 100

The compliance function must be allocated adequate resources and authority according to the size of the institution, its business activities, the complexity of the organisation, and the compliance risk. 101

The institution designates one member of management to be responsible for compliance and thus guarantees the compliance function's unrestricted access to management. 102

The system of remuneration for employees of the compliance function may not contain any incentives which could lead to a conflict of interests. Specifically, remunerations (e.g. salaries, bonuses, fees and premiums) may not be dependent on the performance of individual products and transactions. 103

The compliance function may be merged with other functions (for instance, legal services or risk control) as long as this does not give rise to a conflict of interest; however, the duties and responsibilities of each function must be clearly defined and assigned. 104

Specifically, if the business model and the institution's organisation are not very complex and if the risk of non-compliance is low, the compliance function may also be fulfilled by an individual in a part-time position or in combination with another, non-conflicting function. It may also be outsourced. **105**

If a small institution, due to its size, cannot fully guarantee the required independence (margin no. 100) of its compliance function and the absence of conflicts of interest (margin no. 105), it must find another solution to guarantee the reliability of the compliance function. The audit firm must assess this and state its opinion on this matter in its regulatory audit report. **106**

b) Duties and responsibilities

An internal directive should define the tasks, responsibilities and reports generated by the compliance function; it must be approved by management or the board of directors. The compliance function generally encompasses the following tasks: **107**

- it supports and offers consulting services to management as well as employees in the implementation and supervision of compliance issues; **108**
- at least once a year, it assesses the compliance risks of the institution's business activity, and draws up a risk-oriented activity plan which must be approved by management. This activity plan must also be put at the disposal of internal audit. **109**
- it supports management in training and informing employees in matters of compliance. **110**
- it reports material changes in the assessment of the compliance risks to management in a timely manner, finds and investigates serious cases of non-compliance and supports management in its choice of instructions and counter-measures; internal audit must be informed accordingly. **111**
- once a year, it reports to the board of directors its assessment of the compliance risks and the activities of the compliance function (margin nos. 108–111). A copy of the report must be put at the disposal of internal audit and the audit firm each. **112**

E. Risk Control

a) Implementation and assignment

Each institution maintains a risk control function which has unrestricted access to information, locations and documents with the scope of its function; it must be independent from profit-generating business activities and incorporated into the overall organisation. **113**

Risk control must be allocated adequate resources and authority corresponding to the size of the institution, its business activities, the complexity of its organisation, and the compliance risk. **114**

The institution designates one member of management to be responsible for risk control and thus, guarantees risk control's unrestricted access to management. **115**

Depending on the different risk categories of the institution (e.g. market, credit and operational risks), separate departments may perform risk control tasks; however, all must report to the member of management responsible for risk control. **116**

The system of remuneration for employees of risk control may not contain any incentives which could lead to a conflict of interests. Specifically, remuneration (e.g. salaries, bonuses, fees and premiums) may not be dependent on the performance of individual products and transactions. **117**

The risk control department may be merged with another internal function (for instance, compliance) as long as this does not give rise to a conflict of interest; however, the duties and responsibilities of each function must be clearly defined and assigned. **118**

Specifically, if the business model and the institution's organisation are not very complex and if the risk of non-compliance is low, risk control may also be fulfilled by an individual in a part-time position or in combination with another, non-conflicting function. **119**

If a small institution, due to its size, cannot fully guarantee the required independence (margin no. 113) of risk control and the absence of conflicts of interest (margin no. 119), it must find another solution to guarantee the reliability of risk control. The audit firm must assess this and state its opinion on this matter in its regulatory audit report. **120**

b) Duties and responsibilities

As a rule, an internal directive should define risk control's tasks, responsibilities and reports; it must be approved by management or the board of directors. **121**

As an independent, controlling function, risk control supervises the risk profile of the institution. It prepares the risk information necessary for monitoring risks and lays the cornerstone for the institution's risk policy, its risk appetite as well as its risk limits, all of which must be approved by management or the board of directors. **122**

Risk control is specifically responsible for the design and implementation of an adequate system of risk supervision and its constant adjustment to new business lines and products; the framework and implementation of principles and methods for assessing risks (e.g. valuation and aggregation methods, validation of models) as well as the supervision of adequate systems to assess the requirements regarding capital adequacy, large exposures and liquidity. **123**

Risk control reports risks and risk items to management at least every six months. In the case of unusual developments, it informs management and internal audit immediately. **124**

According to margin nos. 122–124, risk control informs the board of directors of the institution's risk situation and its activities at least once a year. A copy of the report must be put at the disposal of both internal audit and the audit firm. **125**

c) Delineation from risk management

The purpose of risk management is the comprehensive and systematic control and handling of risks on the basis of economic and statistical knowledge. Risk management comprises identifying, measuring, assessing, managing and reporting on individual or aggregates of risk items. Risk management occurs on the appropriate organisational levels, with methods that are adequate for and which reflect the particularities of the institution. **126**

VI. Review and Assessment by the Audit Firm

The bank law audit firm audits the institution's adherence to the stipulations specified in this circular taking into account SFBC circular 05/1 Audit; it records its findings in an audit report (SFBC circular 05/2 Audit Report) **127**

VII. Effective Date

The effective date of this circular is 1 January 2007. **128**

It replaces SFBC circular 95/1 Internal Audit dated 14 December 1995 and the Swiss Bankers Association's guidelines on internal control of June 2002. **129**

VIII. Transitional Provisions

The institutions must fulfil the requirements of this circular no later than 1 January 2008. Regarding the requirements of independence of the members of the board of directors and the audit committee, a transitional grace period is granted until 1 January 2009. **130**

Legal basis

- BA: Art. 3 para. 2 lit. a; Art. 3b h; Art. $4^{quinquies}$
- BO: Art. 8 para. 2, Art. 9; Art. 44 lit. o
- Capital Ordinance: Art. 6–11
- SESTA: Art. 10 para. 2 lit. a; para. 5; Art. 14
- SESTO: Art. 19; Art. 20; Art. 26; Art. 29 para. 1
- SESTO-SFBC: Art. 8 para. 1