KPMG

FINMA circular 2008/21 Operational Risks – Banks

Capital adequacy requirements and qualitative requirements for operational risks at banks

dated 27 March 2014

FINMA circular 2008/21 Operational Risks – Banks

Capital adequacy requirements and qualitative requirements for operational risks at banks

dated 27 March 2014

1 Table of Contents

2 Other Languages

DE: Operationellen Risiken Banken vom 27.3.2014

FR: Risques opérationelles - banques du 27.3.2014

Unofficial translation issued in January 2016

FINMA circular 2008/21
Operational Risks – Banks

Capital adequacy requirements and qualitative requirements for operational risks at banks

Reference:	FINMA circular 08/21 "Operational Risks – Banks"
Issued:	20 November 2008
Entry into force:	1 January 2009
Last amendment:	27 March 2014 [amendments are denoted with an * and are listed at the end of document]
Concordance:	previously FINMA circ. 06/3 "Operational Risks" of 29 September 2006
Legal bases:	FINMASA Article 7(1)(b) BA Article 3(2)(a) and (b), 3g, 4(2) and (4), 4bis(2) BO Article 12 SESTA Article 10(2)(a) SESTO Articles 19(3), 20(1), 29 CAO Articles 2, 89-94 FINMA-FO Article 5 et seqq.
Appendix 1:	Categorization of Business Lines pursuant to Article 93(2) CAO
Appendix 2:	Overview on the Categorization of Event Types
Appendix 3:	Handling of electronic client data

Addressees

BA			ISA			SESTA		CISA									AMLA			OTHERS	
Banks	Financial groups and congl.	Other intermediaries	Insurers	Insurance groups and congl.	Insurance intermediaries	Stock exchanges and participants	Securities dealers	Fund management companies	SICAVs	Limited partnerships for CISs	SICAFs	Custodian banks	Asset managers CIS	Distributors	Representatives of foreign CIS	Other intermediaries	SROs	DSFIs	SRO-supervised institutions	Audit firms	Rating agencies
X	X						X														

Table of Content

Table of Content

I. Object

This Circular shall concretize Articles 89-94 of the Capital Adequacy Ordinance (CAO; SR 952.03) and defines the basic qualitative requirements for the management of operational risk as per Article 12 BO and Articles 19-20 SESTO. In the quantitative area, it shall specify how to determine the capital requirements for operational risk according to the three available approaches, as well as the obligations concomitant with them. The basic qualitative requirements shall correspond to the Basel Principles for the Sound Management of Operational Risk. 1*

II. Definition

According to Article 89 CAO, operational risk shall be defined as "the risk of loss, resulting from the inadequacy or failure of internal processes, people or systems or from external events". This definition shall comprise legal risk, including regulatory fines and settlements, but excludes strategic and reputational risk. 2

Pursuant to Article 89 CAO, reputational risk shall be excluded from the definition of operational risk, since it is usually hard to quantify, if at all. Nevertheless, it should be noted that if operational risk actually materializes, it may have an indirect and potentially serious impact on the bank's reputation. 2.1*

III. Capital adequacy requirements

A. The Basic Indicator Approach (BIA, Article 92 CAO)

Banks using the Basic Indicator Approach to determine their capital requirements must hold capital for operational risk equal to the product of the multiplier α and the average of the earnings indicators GI over the three previous years. To determine the average, only years with positive GI[1] values are to be taken into account. 3

The three previous years mentioned in margin no. 3 (and margin no. 24) shall correspond to the three one-year periods prior to the effective date of the last published income statement. If, for example, the last published income statement was prepared as at 30 June 2008, then the three one-year periods to be taken into account would correspond to the periods from 1 July 2005 until 30 June 2006, 1 July 2006 until 30 June 2007 and 1 July 2007 until 30 June 2008. 4

The required capital K_{BIA} shall be calculated as follows: 5

$$K_{BIA} = \alpha \cdot \sum_{j=1}^{3} \frac{\max[0, GI_j]}{\max[1, n]}$$

[1] In the revised Basel Minimum Standards Framework ("International Convergence of Capital Measurements and Capital Standards – A Revised Framework / Comprehensive Version") of June 2006, the earnings indicator shall be referred to as "Gross Income".

where

- α shall always be set at 15%; 6
- GI_j = earnings indicator for the year j; and 7
- n = number of the three previous years for which the earnings indicator GI was positive. 8

The earnings indicator GI shall be defined as the sum of the following positions from the income statement according to margin no. 125 et seqq. FINMA circ. 15/1 "Accounting – Banks": 9*

- gross interest income (margin no. 131 FINMA circ. 15/1 "Accounting – Banks"); 10*
- commission and fee income[2] (margin no. 139 FINMA circ. 15/1 "Accounting – Banks"); 11*
- results from trading operations and the fair-value option (margin no. 140 FINMA circ. 15/1 "Accounting – Banks"); 12*
- direct investment income (margin no. 143, FINMA circ. 15/1 "Accounting – Banks") of equity shares that need not be consolidated; and 13*
- income from real estate (margin no. 144, FINMA circ. 15/1 "Accounting – Banks"). 14*

The earnings indicator GI at a consolidated level shall be calculated using the same scope of consolidation as shall be used to determine the capital requirements. 15

If a bank's structure or activities are extended (e.g. following the take-over of a new business entity), the historical values of the earnings indicator GI shall be increased accordingly. Downward adjustments of the historical values of the earnings indicator GI (e.g. following the disposal of a business line) have to be approved by the FINMA. 16

To determine the earnings indicator GI pursuant to Article 91(1) CAO, banks may use internationally recognized accounting standards in place of the Swiss accounting standards, subject to approval by the FINMA (cf. Article 91(4) CAO). 17

All income generated from outsourcing agreements in which the bank acts as service provider must be considered as a component of the earnings indicator GI (cf. Article 91(2) CAO). 18

[2] The consideration of commission expenses pursuant to margin no. 138 FINMA circ. 15/1 "Accounting banks" shall be subject to the restrictions of margin no.18.

If the bank acts as principal for an outsourced service, the corresponding expenses may only be deducted from the earnings indicator GI if the services are outsourced within the same financial group and are accounted for on a consolidated basis (cf. Article 91(3) CAO). 19

Repealed 20*

Repealed 21*

Repealed 22*

B. The Standardized Approach (SA, Article 93 CAO)

a) Mechanism

To determine their capital requirements, banks must allocate all of their activities to the following business lines: 23

i	Business line	β_i
1	Corporate finance / advisory	18%
2	Trading and sales	18%
3	Retail banking	12 %
4	Commercial banking	15 %
5	Payment and settlement operations	18 %
6	Custodial and fiduciary transactions	15 %
7	Institutional asset management	12 %
8	Retail brokerage	12 %

Table 1

For each business line i and each of the three preceding years as per margin no. 4 an earnings indicator GI pursuant to margin nos. 9-18 has to be determined and multiplied by the relevant factor β_i in accordance with Table 1. The resulting figures shall first be added for each individual year j. In doing so, negative figures from business lines can be netted with positive figures from other business lines. The capital requirements shall equal the three-year average. When calculating the average, any negative summands are to be set to zero (see Article 93(1) CAO). 24

The capital requirements in the Standardized Approach K_{SA} shall be calculated as follows: 25

$$K_{SA} = \frac{1}{3} \cdot \sum_{j=1}^{3} \max\left[0, \sum_{i=1}^{8} GI_{i,j} \cdot \beta_i\right]$$

where

- $GI_{i,j}$ = earnings indicator in the given relevant year j, for business line i; and 26
- βi shall be a multiplier, identical for all banks, given as fixed percentage for business line i. 27

b) General Requirements (Article 93(3) CAO)

Repealed 28*

In accordance with Appendix 1, every bank must have principles for allocating its business activities to the standardized business lines listed in margin no. 23. For this purpose, it must dispose of documented criteria. The criteria are to be reviewed regularly and must be adjusted to reflect any changes in the bank's activities. 29

c) Repealed

Repealed 30*

Repealed 31*

Repealed 32*

Repealed 33*

Repealed 34*

Repealed 35*

Repealed 36*

Repealed 37*

Repealed 38*

Repealed 39*

Repealed 40*

Repealed 41*

Repealed 42*

Repealed 43*

Repealed 44*

C. Institution-specific Approaches (AMA, Article 94 CAO)

a) Approval

The institution-specific approaches (Advanced Measurement Approaches, AMA) allow banks to quantify capital requirements for operational risk according to their own procedure, provided they meet specific requirements. 45

Applying an institution-specific approach requires the FINMA's approval. 46

Before granting final approval, the FINMA can request banks applying for an institution-specific approach to run parallel calculations based on the approach in question for testing and comparison purposes for a maximum period of two years. 47

A bank using an institution-specific approach can only fully or partially revert to the Basic Indicator or Standardized Approach if the FINMA orders or allows it to do so. 48

Expenses incurred by the FINMA in connection with the approval process and any necessary audit work subsequent to the approval must be borne by the bank. 49

b) Additional Qualitative Requirements

Banks using an institution-specific approach must comply with the basic qualitative requirements set out in chapter IV.B. 50*

In order to use an institution-specific approach for the calculation of capital requirements for operational risk, banks must also satisfy the following additional qualitative requirements. 51

The governing body for the guidance, supervision and control must be actively involved in the oversight of the approach's use. 52

The executive board must be familiar with the basic concepts of the approach and be in a position to exercise their corresponding oversight function. 53*

Banks must have an operational risk management system that is conceptually sound, reliable and implemented with integrity. 54

Banks must dispose of sufficient resources for the management, control and internal audit of the institution-specific approach at all levels of the bank. 55

Banks must have an independent and central operational risk management unit that is responsible for the design and implementation of principles for the management of operational risk. This unit shall be responsible for: 56

- defining institution-wide policies and procedures concerning the management and control of operational risk; 57
- the design and implementation of the institution-specific operational risk measurement methodology; 58
- the design and implementation of a reporting system for operational risk; and 59
- the development of strategies to identify, measure, monitor, as well as control and/or mitigate operational risk. 60

The institution-specific operational risk measurement system must be closely integrated into the bank's day-to-day risk management processes. 61

The output of the institution-specific measurement system must be an integral part of the monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in management reports, for internal capital allocation and for risk analyses. 62

Banks must have methods for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the institution. 63

Repealed 64*

Internal and external auditors must regularly review the operational risk management processes and the implementation of the institution-specific approach. These reviews must include both the activities of the individual business units and of the central operational risk management unit. 65

The audit firm's validation of the operational risk measurement system must in particular include the following: 66

- Verifying that the internal validation processes operate satisfactorily; and 67
- Making sure that data flows and processes associated with the institution-specific approach are transparent and accessible. In particular, it is necessary that the institution's internal and external auditors and the FINMA can access the approach's specifications and parameters. 68

c) General Quantitative Requirements

In line with the Basel minimum standards framework[3], the FINMA does not specify a certain approach but instead leaves banks considerable freedom in this regard. This circular shall therefore be limited to giving the key requirements that have to be met to qualify for using such an approach. The review of detailed specifications for an institution-specific approach shall be part of the individual approval process. The latter shall be headed by the FINMA and include the external auditor. 69

Independently of the specific design of their approach, a bank must be able to demonstrate that it also captures severe loss events occurring with low probability. The resulting capital required for operational risk should approximately correspond to the 99.9%-quantile of the distribution function of the respective aggregate operational risk losses over one year. 70

All institution-specific approaches must base themselves on a definition of operational risk that is in accordance with Article 89 CAO and margin no. 2. In addition, they must also allow a categorization of loss events in accordance with Appendix 2. 71*

[3] Cf. footnote 1.

Capital requirements shall apply to both expected and unexpected losses. The FINMA may grant a bank reliefs for its capital requirements if it holds adequate provisions for future expected losses. 72

All explicit and implicit assumptions regarding dependencies between operational risk loss events as well as between used estimators must be plausible and substantiated.. 73

Each approach shall satisfy certain basic properties. In particular, it shall satisfy the requirement to incorporate the following: 74

- internal loss data (margin nos. 76-85);
- relevant external loss data (margin nos. 86-88);
- scenario analyses (margin nos. 89-91); and
- business environment and internal control factors (margin nos. 92-97).

Banks shall have a reliable, transparent, well-documented and verifiable concept for the inclusion and determination of the relative importance of these four input factors in their overall approach. The approach must be internally consistent and in particular avoid counting risk-mitigating factors more than once (e.g. business environment and internal control factors or insurance contracts). 75

d) Internal Loss Data (Article 94(2) CAO)

A bank must have documented processes to assess the continuous relevance of historical loss data. In particular, this must include clearly defined internal rules on how the consideration of loss data can be altered (e.g. full non-consideration due to a lack of current relevance, scaling due to changed size ratios or other adjustments). The documented processes are also to define who is authorized to make such alterations and up to what degree. 76

A bank must use an internal loss database. When the bank first uses the approach for regulatory purposes, this database shall cover at least three years of historical data. At the latest after two years after first using the approach, the period observed must cover at least five consecutive years. 77

The process for the setup of an internal operational risk loss database must meet the following criteria: 78

- To assist the regulatory validation, a bank must be able to map all of its internal loss data to the business lines in accordance with margin no. 23 and to the event types in accordance with Appendix 2. It shall maintain documented and objective criteria for this categorization. 79*
- The bank's internal loss data must be captured through a robust and sound process. This data must cover all material activities and exposures, including all relevant sub-systems and geographic locations. Banks do not need to systematically collect data on losses below a certain threshold. This gross minimum amount shall be defined by the FINMA. 80

- For each loss event, the bank should collect the following information: gross loss amount, date of the loss event, and any recoveries of the gross loss amount (e.g. from insurance contracts). For loss events with a gross loss amount above CHF 1 million, the causes for the loss event must also be documented. 81

- A bank must define principles for the collation of loss event data. This shall also include criteria for categorizing loss events in a central function (e.g., an information technology department) or loss events that affect more than one business line. In addition, it must be specified how to handle a series of loss events that are not independent from each other. 82

Operational risk losses that arose in the context of credit risk and that the bank historically captured as credit risk may continue to be treated exclusively as credit risk events for the purposes of calculating required capital. However, such losses must nevertheless be included in the internal operational risk loss database if above the FINMA-defined threshold, and be considered for the management of operational risks. Such losses have to be captured similarly to other internal losses, but in respect of operational risks they are to be flagged as irrelevant for capital adequacy purposes. 83

For a loss due to operational risk that also results in a market risk loss, the relevant event shall be captured like other operational risk loss events and to be integrated into the institution-specific approach. A bank applying a risk aggregation model in accordance with margin nos. 228-365 of FINMA circ. 08/20 "Market risks - banks" to determine its capital requirements for market risk may not exclude positions resulting from operational risk events from the value-at-risk calculation, the stress-based value-at-risk calculation, the incremental risk charge, the comprehensive risk measure, or from back-testing. 84*

Negative losses (e.g. gains from a wrongly bought stock position) may not result in lower capital requirements in the institution-specific approach. 85

e) External Loss Data (Article 94(2) CAO)

Banks must include relevant external loss data in their institution-specific approach in order to ensure the consideration of rare, yet potentially severe loss events. Publicly available and/or pooled industry loss data can serve as sources for this relevant information. 86

The external loss data must include actual loss amounts, information on the scale of activities in the affected business area, information on the causes and circumstances of the loss events and information allowing the assessment of the relevance of the loss event for one's own bank. 87

Banks must have a systematic and documented process on how they use external loss data. This particularly includes a clear methodology for the incorporation of this data into their institution-specific approach (e.g. scaling, qualitative adjustments, or influence on scenario analysis). The conditions and practices for the use of external loss data must be reviewed regularly, both internally and by the external audit firm. 88

f) Scenario Analysis (Article 94(2) CAO)

Institution-specific approaches must take into account outcomes from scenario analyses. 89

Scenario analyses, building on expert opinion in conjunction with external data, must assess the bank's exposure to potentially severe loss events. 90

The scenarios used for the scenario analyses and their associated parameters are to be reviewed and, if necessary, adjusted, in the event of a major change to the risk exposure (and at least on an annual basis) to determine whether they are up-to-date and relevant. In case of a significant change to the risk situation, adjustments must be made immediately. 91

g) Business Environment and Internal Control System (Article 94(2) CAO)

As a forward-looking element, a bank's institution-specific approach must use predictive factors from its business environment and internal control system. These factors serve to specifically reflect the current characteristics of the bank's risk profile (e.g. new business activities, new IT solutions, changed processes) or new developments in its environment (e.g. situation in terms of security policy, changes in court practices, exposure to IT viruses). 92

For business environment and internal control factors to qualify for use as part of an institution-specific approach, they must meet the following requirements: 93

- Based on the experience and assessment of the affected business areas, each factor shall be a relevant risk driver. Ideally, the factor should be quantifiable and verifiable. 94

- The sensitivity of a bank's risk estimates to changes in the factors and their relative importance needs to be justifiable and comprehensible. In addition to capturing changes in the risk profile due to improvements in the control environment, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume. 95

- The framework, choice and use of individual factors, including the principles used for any adjustments to empirical estimates, must be documented. The documentation should also be subject to independent review within the bank. 96

- The processes, their results and the adjustments undertaken shall be regularly compared to the actual internal and external loss experience. 97

h) Risk Mitigation through Insurance

When using an institution-specific approach, banks shall be allowed to recognize the risk-mitigating impact of insurance contracts when determining the capital requirements for operational risks. The impact of the risk mitigation shall be limited to a maximum reduction by 20% of the required capital calculated using an institution-specific approach. 98

The option to reduce the required capital shall depend on compliance with the following criteria: 99

- The insurer shall have a long-term credit rating of class 3 or better. The credit rating must come from a rating agency recognized by the FINMA. 100

- The insurance contract must dispose of an initial duration of at least one year. Once the residual term sinks below one year, the risk-mitigating impact shall decrease in a linear manner, from 100% (for a residual term of at least 365 days) to 0% (for a residual term of 90 days). For the determination of capital requirements, no risk mitigating impact shall be recognized from insurance contracts with a residual term of 90 days or less. 101

- The insurance contract shall dispose of a cancellation period of at least 90 days. Once the cancellation period sinks below one year, the risk-mitigating impact shall decrease in a linear manner from 100% (for a cancellation period of at least 365 days) to 0% (for a cancellation period of 90 days). These reduction rates are to be applied on top of any risk-mitigating impacts already reduced due to margin no. 101. 102

- The insurance contract must not have any exclusion or limitation clauses in case of a supervisory intervention or the bank's insolvency that could preclude the bank, its potential buyer, restructuring agent or liquidator from insurance benefits. However, such exclusion or limitation clauses shall be permissible if they restrict themselves exclusively to events occurring after the initiation of bankruptcy proceedings or after liquidation. 103

- The calculation of the risk-mitigating impact from the insurance contracts must be transparent. It must be consistent with the probability and severity of a potential loss event used in the institution-specific approach. 104

- The insurer must be a third-party entity and may not be part of the same group as the bank. If it is part of the same group, the risk-mitigating impact may only be recognized if the insurer cedes the risk exposure to an independent third-party entity (e.g. a reinsurer) that in turns meets all the eligibility criteria for an insurer. 105

- The bank's internal concept for recognizing insurance must be based on the effective transfer of risk. It must be well documented. 106

- The bank must disclose information on its use of insurance for the mitigation of operational risk. 107

D. Partial Use of Approaches

In principle, it shall be permissible to limit the use of an institution-specific approach to individual areas of activity, and cover remaining areas through the Basic Indicator Approach or the Standardized Approach, provided that the following conditions shall be met: 108

- All of the bank's operational risks must be captured by one of the approaches described in this circular. In doing so, the respective requirements for these approaches have to be met in the corresponding areas of activity. 109

- At the time of application of an institution-specific approach, the approach must capture a significant part of the bank's operational risks. 110

- A bank must have a timeline for the rollout of its institution-specific approach across all of its significant legal entities and business lines. 111

It is not permissible to retain the Basic Indicator or Standardized Approach in selected significant areas of activity in order to minimize capital requirements. 112

The delineation between the institution-specific approach and the Basic Indicator or Standardized Approach can be based on business lines, legal structures, geographical boundaries, or other internally clearly defined delineation criteria. 113

Except for cases listed in margin nos. 108-113, it is not permissible to use different approaches to determine capital requirements for operational risks. 114

E. Adjustment to Capital Requirements (Article 45(3) CAO)

As part of its supervisory function regarding additional capital, the FINMA shall be in a position to increase the capital requirements for individual banks (Article 45 CAO). Such individual increases of capital requirements in particular impose themselves if a determination of capital requirements exclusively based on the Basic Indicator or Standardized Approach would lead to inappropriately low capital requirements due to low earnings indicators GI. 115

F. Minimum Capital and Lower Limit (Floor)

In application of the continued "floor regime" published by the Basel Committee, the following applies[4]: For banks calculating capital requirements for operational risk according to the AMA, the minimum capital requirements at overall bank level, taking into account deductions from the eligible capital, cannot be lower than 80% of the requirements and deductions that the bank would have had if it had applied the Basel I minimum standard.[5] 116*

In application of Article 47 CAO, the FINMA stipulates for each institution how it should perform an adequate approximate calculation of the theoretical Basel I requirements. For operational risk, it refers to the standard approach as described in Article 93 CAO.

IV. Qualitative Requirements

A. Principle of Proportionality

The requirements set out in this chapter are to be implemented depending on the bank's size. Margin no. 119 lists the margin numbers from which small banks shall be exempted. 117*

[4] Cf. press release of the Basel Committee of 13 July 2009: www.bis.org/press/p090713.htm

[5] This shall be equivalent to the calculation of capital requirements as per the Banking Ordinance of 17 May 1972 that was valid until 31 December 2006 (AS **1995** 253, **1998** 16).

Small banks as per margin no. 117 shall be: 118*

- banks in FINMA category[6] 5
- Securities dealers in FINMA categories 4 and 5
- In some cases also banks in FINMA category 4, on grounds of their type, their scope, their complexity and the riskiness of their business activities. The institute-specific assessment of whether the criteria are fulfilled shall be principally done by the bank itself and its audit firm. The bank's and audit firm's assessments must be documented transparently and in a manner understandable to a third party.

B. Basic Qualitative Requirements

Small banks as described in margin nos. 117 and 118 shall be exempt from requirements stipulated in margin nos. 125, 126, 129, 130, 132, 133 and 134. 119*

The basic qualitative requirements shall be based on the Principles for the Sound Management of Operational Risk issued by the Basel Committee on Banking Supervision (June 2011). 120*

a) Principle 1: Responsibilities

The governing body for the overall management, supervision and control (hereinafter: board of directors) must approve and regularly review a framework for the management of operational risks, which specifically defines the risk appetite and risk tolerance. As part of this, the type and level of operational risks to which the bank is exposed and which it is willing to take must be documented. 121*

Executive Management or a committee led by a member of Executive Management must develop this framework, translate it into specific guidelines and processes and then implement it in the business units' risk management processes in a manner that is verifiable. In this, measures must be included to identify and remedy violations of risk appetite and risk tolerance in a timely manner. 122*

Executive Management must define unambiguous and effective responsibility structures for the management of operational risks. As part of this, an organizational unit shall be designated to be responsible for the framework's maintenance and ongoing development to manage operational risks. This organizational unit must have sufficient qualified staff to effectively carry out its responsibilities. Like other risk management units, the organizational unit for the management of operational risks must be adequately represented in the bank's relevant committees. 123*

Executive Management shall be responsible for ensuring that the framework is consistently applied and maintained at the level of all new and key existing products, activities, processes and systems. 124*

[6] cf. appendix of the FINMA circ. 11/2 "Capital buffer and capital planning - Banks".
[7] www.bis.org/publ/bcbs195.pdf

b) Principle 2: Framework and Control System

The framework must be adequately described in the internal regulations approved by the Board of Directors and must contain bank-specific details based on regulatory definitions of operational risk and operational losses.[8] 125*

The framework must cover at least the following aspects: 126*

a. structures for the management of operational risk, including competencies, accountabilities and reporting lines;

b. definition and use of instruments for identifying, assessing and controlling operational risk;

c. definition of risk appetite and risk tolerance in regard to the relevant types of operational risk; definition of thresholds and/or limits; definition of risk mitigation strategies and instruments;

d. the bank's approach to identify inherent risks (risks before taking into account any controls) and to determine and monitor thresholds and/or limits for residual risks (the risks remaining after taking into account controls);

e. definition and establishment of risk reporting and management information systems (MIS) for operational risk;

f. definition of a standardized classification of significant operational risks to guarantee consistency in risk identification, risk valuation and objectives of the operative risk management;[9]

g. structuring of the documentation which enables an appropriate and independent review and assessment of operational risks;

h. duty to engage in timely checks and adjustments in case of significant changes to the risk situation.

Banks must dispose of an adequate, documented control system that is based on guidelines, processes and systems. Moreover, they must implement internal controls and adequate risk mitigation and/or risk transfer strategies. 127*

c) Principle 3: Identification, Mitigation and Monitoring

The identification, mitigation and monitoring of risks form the foundation of an effective risk management system. An effective risk identification, which forms the basis for the limitation and monitoring of operational risk, shall take both internal[10] and external[11] factors into account. These shall include at least risk and control assessments as well as audit findings. 128*

[8] Operational losses denote losses resulting from the inadequacy or failure of internal processes, people or systems, or from external events. This includes legal risks, but excludes strategic and reputational risks (Article 89 CAO).

[9] If there is no standardized classification of operational risks, this may increase the likelihood that risks are not identified and categorized or that the responsibilities for the assessment, supervision, control and mitigation of risks are not allocated.

[10] For example, a bank's corporate structure, type of activities, employee qualifications, organizational changes and staff fluctuations.

[11] For example, changes to the bank's larger environment and the industry as such, as well as technological developments.

Depending on the institute-specific business activities and their nature, scope, complexity and risk, additional tools and methods should be considered and applied, where appropriate: 129*

a. collection and analysis of internal loss data;

b. collection and analysis of external events with operational risks;

c. analysis of linkages between risks, processes and controls;

d. risk and performance indicators used to monitor operational risks and indicators for the effectiveness of the internal control system;

e. scenario analyses;

f. estimate of the loss potential;

g. comparative analyses[12]

The organizational units entrusted with the mitigation and monitoring do this using the instruments, structures, approaches, etc. defined in the framework. As an indirect measure for mitigating operational risk, a risk-based internal pricing and performance measurement may also be applied. 130*

d) Principle 4: Internal and External Reporting

Executive Management must implement a process for the continuous monitoring of the bank's operational risk profile and material loss risks. Adequate reporting mechanisms facilitating the proactive management of operational risks must exist at the level of the Board of Directors, Executive Management and the business areas. 131*

The internal reporting of operational risks should include financial, operational and compliance data, but also significant risk-relevant external information on events and conditions. Operational risk reporting must cover at least the following aspects and present their possible consequences for the bank and its operational risk capital: 132*

a. breaches of the bank's defined risk appetite and risk tolerance as well as exceedances of fixed thresholds and/or limits for relevant types of operational risk;

b. details on material internal operational risk events and/or losses;

c. information about external events which may be relevant for the bank, and potential risks and their potential impact on the bank.

A bank must dispose of a formal disclosure policy approved by the Board of Directors, which shows how the bank discloses its operational risk and which disclosure control processes are to be applied. 133*

[12] In a comparative analysis, results from different assessment tools shall be compared in order to obtain a better view on the bank's operational risks.

The data disclosed externally by the bank must allow stakeholders to obtain an understanding of the bank's approach for the management of operational risk. Inter alia, it should include the concept for the management of operational risks. This should enable stakeholders to assess the effectiveness of the identification, mitigation and monitoring of operational risk. 134*

e) Principle 5: Technological Infrastructure

Executive Management must ensure an adequate technology infrastructure which reflects the bank's current and long-term business needs and is able to mitigate operational risk. For this purpose, it must make available sufficient resources that cover both business-as-usual activities and times of stress. Moreover, it must ensure the security, integrity and availability of the data and systems and implement an integrated and comprehensive risk management for the technology infrastructure. 135*

f) Principle 6: Continuity in the Event of a Business Interruption

Executive Management must dispose of business continuity plans for the bank which ensure the continuity of activities and limitation of damage in the event of a serious business interruption.[14] 136*

C. Risk-specific Qualitative Requirements

Specific operational risks with far-reaching implications have to be managed and controlled more comprehensively and intensely than set out by the basic qualitative requirements. Executive Management must situationally define and implement additional, risk-specific measures or tighten existing measures. 137*

If the FINMA deems it to be necessary, it may define the management of operational risk in even more detail for specific areas. This shall be done prudently and using the principle of proportionality. Further qualitative requirements will be published in the Appendix to this circular, sorted by topic. 138*

V. Auditing and Assessment by Audit Firms

Audit firms are to audit the compliance with the provisions of this circular according to the FINMA circ. 13/3 "Auditing" and capture the findings of their audit procedures in the audit report. 139*

[13] Technology infrastructure encompasses both physical and logical (electronic) aspects of IT and communication systems, the individual hardware and software components as well as any data and the operating environment.

[14] cf. the FINMA circular 2008/10 "Self-regulation as a minimum standard" recognized minimum standard items of the SBA recommendations for Business Continuity Management (BCM).

I. Appendix 1

II. Categorization of Business Lines pursuant to Article 93(2) CAO

I. Overview

1st Level	2nd Level	Activities
Corporate finance / advisory	Corporate finance / advisory	Mergers and acquisitions, issuance and placement business, privatizations, securitization, research, loans (public authorities, high-yield), participations, syndications, initial public offerings, private placements in secondary trading
	Public authorities	
	Trade financing	
	Advisory services	
Trading and sales	Customer trading	Bonds, shares, foreign exchange transactions, commodities business, loans, derivatives, funding, proprietary trading, securities loans and repos, brokerage (for non-retail investors), prime brokerage
	Market making	
	Proprietary trading	
	Treasury	
Retail banking	Retail banking	Investment and lending business, services, fiduciary transactions and investment advice
	Private banking	Investment and lending business, services, fiduciary transactions, investment advice and other private banking services
	Card services	Credit cards for corporate and retail clients
Corporate banking	Corporate banking	Project financing, real estate financing, export financing, trade financing, factoring, leasing, granting of credit, guarantees and warranties, exchange business
Payment and settlement operations[15]	External clients	Payment transactions, clearing and securities settlements for third parties

[15] Losses due to payment transactions and securities settlements, which relate to the institution's own activities, must be allocated to the pertinent business line.

Custodial and fiduciary transactions	Custody	Escrow, deposit business, custody, securities lending for clients; similar services for companies
	Trust business	Issuers and paying agents
	Company foundations	
Institutional asset management	Discretionary asset management	Pooled, segmented, retail, institutional, closed, open, private equity
	Non-discretionary asset management	Pooled, segmented, retail, individual, private, individual, institutional, closed, open-ended
Retail brokerage business	Execution of securities orders	Execution, incl. all related services

II. Allocation principles

1. All of a bank's activities must be mapped to one of the eight business lines (1st level in table 2) in an exhaustive manner. The mapping must not lead to overlaps. 2

2. Also, activities of an ancillary nature that are not directly linked to the bank's core business activities must be allocated to a business line. If the support pertains to a business line, the mapping must also be done to this business line. If more than one business line is supported by an ancillary activity, the allocation must be based on objective criteria 3

3. If an activity cannot be mapped to a particular business line based on objective criteria, then it shall be mapped to the business line with the highest β factor.. The same shall apply to any ancillary activities. 4

4. Banks may use internal allocation methods to allocate their earnings indicator GI, provided that the bank's total earnings indicator (as used in the Basic Indicator Approach) equals the sum of earnings indicators for the eight business lines. 5

5. The allocation of activities to different business lines to determine capital requirements for operational risk must in principle be compatible with the delimitation criteria used for credit and market risk. Any deviations of this principle must be clearly justified and documented. 6

6. The entire allocation process must be clearly documented. In particular, the written definitions of the business lines must be clear and detailed enough to allow third parties not familiar with the bank to replicate the business line mapping. Where exceptions to the allocation principles are possible, these must also be clearly justified and documented. 7

7. The bank must dispose of processes that facilitate the mapping of any new activities or products. 8

8. Executive Management shall be responsible for the allocation principles. These are to be approved by the governing body for the overall management, supervision and control. 9*

9. The mapping process shall be subject to regular review by the audit firm. 10

Appendix 2

Overview on the categorization of event types

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
Internal fraud	Losses due to acts with fraudulent intent, misappropriation of property, circumvention of laws, rules or internal regulations (involving at least one internal party)	Unauthorized activity	Unreported transactions (intentional) Unauthorized transactions (with financial loss) Erroneous recording of positions (intentional)
		Theft and fraud	Fraud, credit fraud, worthless deposits Theft, extortion, embezzlement, robbery Misappropriation of assets Malicious destruction of assets Forgery Check fraud Smuggling Unauthorized access to accounts Tax offenses Bribery Insider dealing (not on firm's account)
External fraud	Losses due to acts with fraudulent intent, misappropriation of property or circumvention of laws or rules (not involving an internal party)	Theft and fraud	Theft, robbery Forgery Check fraud
		IT security	Damage by hacking activities Unauthorized data access (with financial loss)

Appendix 2

Overview on the categorization of event types

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
Workplace	Losses arising from violations of labor, safety or health regulations and arrangements, including all payments made in the context of such violations	Employees	Compensation and severance payments, losses arising in connection with strikes, etc.
		Occupational safety	General liability Breach of health and safety rules Compensation or indemnity payments to employees
		Discrimination	Indemnity payments for discrimination claims
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet an obligation to a client, or from the nature or structure of a product	Duties of suitability, disclosure & fiduciary duties	Breaches of fiduciary duties, violations of guidelines Issues in regard to suitability or disclosure (know-your-customer rules, etc.) Violation of information requirements Violation of banking client confidentiality or data protection regulations Aggressive sales practices Inappropriate generation of commissions and brokerage fees Misuse of confidential information Lender liability

Appendix 2

Overview on the categorization of event types

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
		Improper business or market practices	Breach of antitrust rules Unfair market practices Market manipulation Insider dealing (on firm's account) Unauthorized business activities Money laundering
		Problems with products	Product issues (e.g. lack of authority, etc.) Model errors
		Client selection, inappropriate business placement and credit exposure	Client evaluations not compatible with internal guidelines Limit exceedances
		Advisory activities	Disputes in relation to results from advisory activities
Damage to physical assets	Losses arising from damage to physical assets due to natural disasters or other events	Catastrophes or other events	Natural disasters Terrorism Vandalism
Business interruptions and system failures	Losses arising from business disruptions or issues with technical system	Technical systems	Hardware Software Telecommunication Power failures, etc.

Appendix 2

Overview on the categorization of event types

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
Execution, delivery and process management	Losses arising from erroneous business processing or process management, from relations with business partners, vendors, etc.	Transaction capture, execution and maintenance	Communication errors Errors in data capturing or data maintenance Missed deadlines Non-fulfillment of a task Errors in model use or system application Accounting errors or allocation to the wrong unit Erroneous delivery or non-delivery Flawed hedge management Incorrect use of reference data Errors in other tasks
		Monitoring and reporting	Non-fulfillment of reporting obligations Inadequate reports to external parties (causing losses)
		Client onboarding and documentation	Non-compliance with internal and external regulations
		Client account management	Granting of non-authorized access to accounts Incorrect client account management (causing losses) Loss or damage of client assets due to negligent actions

Appendix 2

Overview on the categorization of event types

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
		Business partners Vendors and suppliers	Faulty service from a business partner (non-client) Various disputes with business partners (non-client)
			Outsourcing Disputes with vendors and suppliers

Appendix 3*

Handling of electronic client data

This appendix shall set out the principles and corresponding explanations on the proper management of risks related to the confidentiality of electronic personal data of natural persons ("private clients"[16]) whose banking business is managed in/from Switzerland ("client data"). These principles shall be mainly tailored to the risk of events relating to the confidentiality of mass client data when using electronic systems. They shall only marginally address security considerations of physical data or questions of data integrity and availability. The relevant legal regulations cannot only be found in supervisory law[17], but also in data protection law[18] and in civil law. 1*

Small banks[19] shall be exempt from fulfilling the following margin nos.: 2*

- margin nos. 15-19, as well as 22 of Principle 3;
- all margin nos. of Principles 4-6;
- margin no. 41 of Principle 7.

I. Principles for the proper management of risks in connection with client data confidentiality

A. Principle 1: Governance

Risks in connection with client data confidentiality must be systematically identified, mitigated and monitored. Executive Management mandates an independent unit to be a control function with the task of creating a framework to secure and maintain the confidentiality of client data. Executive Management entrusts an independent control function with the task of creating a proper framework to secure and maintain the confidentiality of client data. 3*

a) Independence and responsibility

The unit responsible for the creation and maintenance of the framework that secures the confidentiality of client data must be independent of the units responsible for processing the data. 4*

For all functions and locations involved, responsibilities must be regulated and clear escalation structures must be created. Executive Management must specifically define the responsibilities and allocate these to the front office, IT and controlling functions; the Board of Directors must approve these appointments. Executive Management must regularly inform the Board of Directors on the effectiveness of the controls introduced. 5*

[16] "Private clients" also include business relationships where a natural person enters a business relationship with the bank with the help of a legal entity (e.g. as the beneficial owner of a domiciliary company, foundation) or a trust.
[17] Specifically Articles 3 and 47 BA as well as Article 12 BO; Articles 10 and 43 SESTA and Articles 19 et seq. SESTO.
[18] Specifically Article 7 FADP and Article 8 et seqq. OFADP (also see FDPIC guidelines ; available atwww.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de).
[19] Cf. margin no. 118.

b) Guidelines, processes and systems

It is expected that the bank has a formal and comprehensive framework to address activities, processes and systems regarding data confidentiality. This framework's structure should reflect the bank's size and complexity. This framework must be consistently implemented in all functions and units that process or have access to client data. 6*

The measures and their periodicity must be specified in writing and in a comprehensible and binding manner, on the basis of the risk appetite and risk tolerance defined by the bank. 7*

The implementation and adherence to the framework on client data confidentiality must be monitored by the Board of Directors and must be guaranteed by regular controls by the unit responsible for data security and confidentiality. 8*

B. Principle 2: Client Identifying Data (CID)

A basic requirement for an adequate framework to ensure client data confidentiality is the categorization of client data which the institution has to process. This shall require the company-specific definition of client identifying data (CID) and its categorization according to the level of confidentiality and protection required. Moreover, the assignment of data responsibility (data owners) must be defined. 9*

a) Client data categories and definition of CID

The institution must dispose of and formally document a clear and transparent list of client data categories, including the company-specific definition of CID. The categorization and definition of client data must include all direct client identification data (e.g. first name, second name, family name), indirect client identification data (e.g. passport number) and potentially indirect client identification data (e.g. a combination of date of birth, profession, nationality, etc.). 10*

Each bank must dispose of a categorization and company-specific definition of CID appropriate for its own specific client database. 11*

b) Classification of CID and levels of confidentiality

CID must be assigned to levels of confidentiality according to formal classification criteria. The classification of client data used to protect data confidentiality must have clearly defined requirements regarding access and the relevant technical measures (e.g. anonymization, encryption or pseudonymization). Moreover, it must differentiate between the various levels of confidentiality and protection. 12*

c) CID responsibility

The institution must define allocation criteria for data ownership that shall be equally applicable to all units that can access or process CID. Units responsible for CID (data owners) must monitor the entire life cycle of client data, including the approval of access rights as well as the deletion and disposal of all backup and operational systems. 13*

Units responsible for CID (data owners) shall be in charge of implementing data classification guidelines as well as of justifying and documenting exceptions. 14*

C. Principle 3: Data storage location and access to data

The bank must know where CID is stored, which applications and IT systems are used to process CID and from where it can be electronically accessed. Adequate controls must be in place to ensure that data is processed as stipulated in Article 8 et seqq. of the Ordinance on Federal Act on Data Protection (OFADP). Special controls shall be necessary for physical locations (e.g. server rooms) or network zones that store or make accessible large quantities of CID Data access must be clearly regulated and must only take place on a strict "need-to-know" basis. 15*

a) Data storage location and access in general

The bank must have an inventory of its applications that contain or process CID and of the connected infrastructure. This inventory must be continuously updated. 16*

The granularity of the institution's inventory shall allow determining the following: 17*

- where CID is stored, which applications and IT systems process CID and where CID can be accessed electronically (end-user applications); 18*
- from which national and international locations and legal unities data can be accessed (including outsourced services and external firms). 19*

b) Data storage location and access from abroad

If CID is stored outside of Switzerland or if it can be accessed from abroad, associated increased risks with respect to client data protection must be adequately mitigated.[20] CID must be adequately protected (e.g. anonymized, encrypted or pseudonymized). 20*

c) The "*need to know*" principle

Staff may only have access to data or functionalities which are necessary for the execution of their duties. 21*

d) Access rights

The Bank must dispose of an authorization system specific to roles and functions, which unambiguously regulates CID access permissions of employees and third parties. To ensure that only individuals currently authorized have access to CID, permissions must be reconfirmed regularly. 22*

[20] Moreover, the relevant regulations of the data protection law, like Article 6 FADP, must be complied with.

D. Principle 4: Security standards for infrastructure and technology

Security standards for infrastructure and technology that are used to protect the confidentiality of CID must be adequate with regard to the bank's complexity and risk exposure, and ensure the protection of CID at the terminal device (i.e. endpoint), as well as its transfer and storage. As information technologies are subject to rapid developments, developments in regard to data security solutions must be followed attentively. Gaps between the internal framework used to ensure client data confidentiality and market practice must be reviewed regularly. 23*

a) Security standards

The security standards must be appropriate in view of the size and complexity level of the bank's IT architecture. 24*

b) Security standards and market practice

Security standards form an integral part of the framework ensuring client data confidentiality. They should be compared to market practice on a regular basis in order to identify potential security gaps. External inputs in the form of independent reviews and audit reports must also be taken into account. 25*

c) Security during the transfer of CID and for CID stored on a terminal device (endpoint)

In order to ensure the confidentiality of CID, the bank must evaluate protective measures (e.g. encryptions) and, where required, implement these at the following levels: 26*

a. Security of CID on terminal devices or endpoints (e.g. PCs, notebooks, portable data storage and mobile devices); 27*

b. Security during the transfer of CID (e.g. within a network or between various locations); 28*

c. Security of stored CID (e.g. on servers, databases or backup media). 29*

E. Principle 5: Selection, monitoring and training of employees with access to CID

Well-trained and responsible employees are vital for the successful company-wide implementation of measures for the protection of client data confidentiality. Employees with CID access must be selected, trained and monitored carefully. This shall also be true for third parties which may access CID on the bank's behalf. IT super users and other users with functional access to mass CID ("key employees") shall require increased security measures. They must be monitored with particular attention. 30*

a) Careful selection of employees

Employees with access to CID must be carefully selected. Specifically, potential employees must be scrutinized prior to starting their activity to verify whether they fulfill the requirements for adequate handling of CID. The bank must also contractually stipulate in what way to select employees through third parties, as well as employees from third parties, who will access CID on the bank's behalf, in order to have all employees undergo a similarly diligent selection process. 31*

b) Special training for employees

Internal and external employees must be made aware of client data security through targeted training programs. 32*

c) Security requirements

The bank must have clear security requirements for employees with access to CID. It must regularly review whether the requirements for an adequate treatment of CID are still fulfilled. IT super users and other users with functional access to mass CID ("key employees") require increased security measures. 33*

d) List of key employees

In addition to the general requirements in regard to access permissions for employees and third parties (see margin no. 22), the bank shall be expected to keep and continuously update a list of all internal and external IT super users and users that have access to mass CID (key employees) and/or have responsibilities with respect to the controlling and monitoring client data confidentiality. 34*

The bank must introduce measures such as log files in order to facilitate the identification of users who have access to mass CID. 35*

F. Principle 6: Risk identification and control related to CID confidentiality

The unit responsible for data security and confidentiality identifies and evaluates inherent risks and residual risks regarding CID confidentiality using a structured process. This process must comprise risk scenarios[21] CID confidentiality that are relevant for the bank and the definition of the corresponding key controls. The catalog of key controls in regard to data confidentiality applied to protect CID must be reviewed regularly for adequacy and, if necessary, adapted. 36*

a) Risk assessment process

A structured process must be used to assess the inherent risk and the residual risk regarding the confidentiality of CID. The business, IT and control functions must be involved in the assessment. 37*

a) Risk scenarios and key controls[22]

The definition of risk scenarios and relevant key controls regarding the confidentiality of CID must be adequate in view of the bank's risk exposure and complexity, and be revised regularly. 38*

[21] MOn the basis of an analysis of serious incidents in regard to data security which have taken place at the bank itself or at a competitor, or a description of purely hypothetical, serious incidents.

[22] Market practice on security scenarios and the related key controls shall be treated in detail by the Swiss Bankers Association in its document, "Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association" (passed in October 2012).

G. Principle 7: Risk mitigation with regards to CID confidentiality

Identified risks must be monitored and adequately minimized. This pertains in particular to data processing activities as part of which large quantities of CID have to be modified or migrated.[23] In case of structural changes (e.g. significant reorganizations), the bank must address security measures for CID confidentiality early on and in depth. 39*

a) Production environment, data processing activities associated with mass CID

Data processing done in the production environment for mass CID that have not been anonymized, encrypted or pseudonymized must be subject to proper processes (e.g. four-eye principle or log files), including the notification of the unit responsible for data security and confidentiality. 40*

b) Tests for the development, change and migration of systems

CID must be adequately protected against the access and use by unauthorized parties during the development, change or migration of systems. 41*

H. Principle 8: Incidents related to the confidentiality of CID, internal and external communication

Banks shall introduce predefined processes in order to be able to react swiftly to confidentiality incidents, including a clear strategy of how to communicate serious incidents. Moreover, exceptions, incidents and audit results must be monitored, analyzed and shared with top management in an adequate form. Such actions must contribute to the continuous refinement of the measures used to secure the confidentiality of CID. 42*

a) Identification of confidentiality incidents and response

A clearly defined process must be formalized for the identification of incidents with regards to confidentiality as well as for the responses to such incidents. All involved units within the institution are to be notified of this process. 43*

b) Notification

Risks of confidentiality breaches for CID and related compliance statements shall be adequately addressed in the institution's internal reporting. Alternatively, in case of non-disclosure requirements for such incidents, it must be ensured that there is systematic recording and escalation to the relevant offices. 44*

c) Continuous refinement of the framework for securing CID confidentiality

The framework for securing CID confidentiality (margin no. 6, 7 and 8) and the security standards (margin no. 24) must be reviewed regularly. Incidents, exceptions, control and audit results must contribute to the continuous refinement of the framework. 45*

[23] This usually happens in case of the development, change or migration of systems due to technology upgrades or organizational restructuring.

d) External communication

The bank must dispose of a clear communication strategy in case of serious incidents regarding CID confidentiality. In particular, it must address the form and time of notification to the FINMA, the prosecution authorities, the affected clients and the media. 46*

I. Principle 9: Outsourcing services and large orders in regard to CID

When selecting providers of outsourcing services that will be processing CID, the confidentiality of CID must be a decisive criterion and an integral component of the underlying due diligence. According to FINMA circ. 08/7, "Outsourcing – Banks", the bank continues to be ultimately responsible for CID during the entire life cycle of the outsourced services. The following requirements are mandatory for all types of activities that involve the access to mass CID, including large orders (e.g. third-party providers of IT services, support for the installation and maintenance of externally developed IT platforms, hosting of applications, etc.) as well as for non-IT services (e.g. outsourcing of client events, etc.). 47*

a) Due diligence regarding CID confidentiality

Due diligence regarding CID confidentiality must be part of the process when selecting outsourcing services and providers for large orders. Clear criteria must be defined to evaluate security and confidentiality standards of such third parties. The review with regards to CID security and confidentiality standards must be done before the contractual agreement and repeated regularly. 48*

a) Due diligence regarding the confidentiality of CID and service agreements

Third parties must be informed of the bank's internal security and confidentiality standards, as well as possible expansions thereof, and must fulfill these as minimum standards. 49*

b) General responsibility

For each outsourced activity involving access to CID, the bank must define at least one internal employee responsible for the adherence to the security and confidentiality standards regarding CID confidentiality. 50*

c) Design of controls and effectiveness tests

The bank must know and understand which key controls the outsourcing service provider must perform with regards to CID confidentiality. As part of this, adherence to internal requirements as well as the effectiveness of the key controls must be verified and assessed. 51*

II. Glossary

Client Identifying Data (CID) client data that reflect personal data as per Article 3 FADP and make it possible to identify the clients involved. 52*

Mass CID: quantities of CID which in relation to the overall number of accounts/total size of private client portfolios are considered to be significant. 53*

Large orders: all services provided by a third party which require or could potentially lead to the access to mass CID (e.g. during the implementation of access rights profiles by third-party employees). A CID risk could arise in the installation of applications or when implementing local settings (e.g. access rights), when storing data or during the ongoing system maintenance (e.g. third-party vendors of IT services, externally developed IT platforms). This shall also include internal audit work and external audits. Normally, such large orders shall be of a long-term nature. 54*

Third-party employees: all employees who work for a contractor of the bank (e.g. contractors, consultants, external auditors, external support, etc.), have access to CID, and who are not internal employees. 55*

Key employees: all internal and external employees in the IT area as well as other areas of the company who have privileged access to large quantities of CID due to their activity profile and responsibilities (e.g. database administrators, members of senior management). 56*

Serious incident with regards to client data confidentiality / leakage of mass client data: an incident with regards to client data confidentiality implying an important leakage of CID (in comparison to the total number of accounts, total size of the client portfolio). 57*

Key controls: a control which will significantly lower the risk of any breach in CID confidentiality if defined, implemented and executed appropriately. 58*

Inherent risk: risk existing before controls or mitigating measures are taken into account. 59*

Residual risk: risk remaining after taking into account controls and mitigating measures. 60*

Reversible data processing techniques: 61*

- Pseudonymized data (pseudonymization): pseudonymization involves the segregation of identifying data (e.g. name, photo, e-mail address, phone number) and other data (e.g. account balance, credit standing). The link between the two data regions shall be given through so-called pseudonyms and a mapping table (concordance table). For instance, pseudonyms can be produced by a random-number generator and, if needed, allocated to the identifying personal data by means of a concordance table. 62*

- Encrypted data: in practice, pseudonymization shall also be done by means of encryption methods. In this case, the pseudonym shall be produced through encryption of identifying personal data with a cryptographic key. The re-identification shall be done through decryption using the secret key. 63*

Irreversible data processing techniques: 64*

- Anonymized data: when anonymizing personal data, all elements that could allow identification of a person are removed or changed permanently (e.g. through deletion or aggregation) so that the data can no longer be attributed to a specific or determinable person. Such data is no longer considered to be CID and therefore shall not be subject to the DPA.[24] 65*

[24] Cf. FDPIC, Appendix to the Guidelines on the Minimum requirements for a Data Protection Management System, 5.

List of amendments

The circular is amended as follows:

These amendments were passed on 1.6.2012 and enter into force on 1.1.2013.

Amended margin no. 84

The references to the Capital Adequacy Ordinance (CAO; SR 952.03) have also been adapted to the version entering into force on 1.1.2013.

These amendments were passed on 29.8.2013 and enter into force on 1.1.2014.

Newly inserted margin no. 116

These amendments were passed on 29.8.2013 and enter into force on 1.1.2015.

Newly inserted margin nos. 2.1, 117–139

Amended margin nos. 1, 29, 50, 53, 71, 79

Amended margin nos. 20–22, 28, 30–44, 64

Other amendments	new main title before margin no. 3 and restructuring of titles Amended title before margin no. 50

These amendments were passed on 27.3.2014 and enter into force on 1.1.2015.

Amended margin nos. 1, 9, 10, 11, 12, 13, 14

The appendices to the circular were amended as follows:

These amendments were passed on 29.8.2013 and enter into force on 1.1.2015.

The enumeration of the appendices has been adjusted: Appendix 2 "Categorization of Business Lines pursuant to Article 93(2) CAO" is now Appendix 1 and Appendix 3 "Categorization of Types of Loss Events" is now Appendix 2

New	Appendix 3
Repealed	Appendices 1 and 4

Contacts

Philipp Rickert
Partner, Head of Financial Services, Member of the Executive Committee
Zurich
Tel. +41 58 249 42 13
prickert@kpmg.com

Cataldo Castagna
Partner, Financial Services
Zurich
Tel. +41 58 249 52 85
ccastagna@kpmg.com

Michael Schneebeli
Partner, Financial Services
Zurich
Tel. +41 58 249 41 06
mschneebeli@kpmg.com

Patrizio Aggio
Director, Financial Services
Lugano
Tel. +41 58 249 32 34
paggio@kpmg.com

Olivier Gauderon
Partner, Financial Services
Geneva
Tel. +41 58 249 37 56
ogauderon@kpmg.com

Markus Schunk
Partner, Head Investment Management
Zurich
Tel. +41 58 249 36 82
markusschunk@kpmg.com

Jürg Birri
Partner, Leiter Regulatory Competence Center
Zurich
Tel. +41 58 249 35 48
jbirri@kpmg.com

Mirko Liberto
Partner, Financial Services
Zurich
Tel. + 41 58 249 40 73
mirkoliberto@kpmg.com

Manfred Suppan
Director, Financial Services
Zurich
Tel. +41 58 249 57 98
msuppan@kpmg.com

www.kpmg.ch