KPMG

Circular 2008/21 Operational Risk – Banks

Capital adequacy requirements and qualitative requirements for operational risks at banks

dated 31 October 2019

Circular 2008/21
Operational Risk – Banks

Capital adequacy requirements and qualitative requirements for operational risks at banks

dated 31 October 2019

1 Table of Contents

2 Other Languages

DE: FINMA-RS 2008/21 Operationelle Risiken Banken 31.10.2019

FR: Circ. FINMA 2008/21 Risques opéerationnels - banques 31.10.2019

Unofficial translation issued in March 2020

Circular 2008/21
Operational Risk – 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:	31 October 2019 [amendments are denoted with an * and are listed at the end of the 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.
Annex 1:	Categorization of Business Lines pursuant to Article 93(2) CAO
Annex 2:	Overview on the Categorization of Event Types
Annex 3:	Handling of Electronic Client Data

Addressees

BA			ISA				SESTA	FMIA						CISA										AMLA			OTHERS	
Banks	Financial groups and congl.	Other intermediaries	Insurance companies	Ins. groups and congl.	Distributors		Securities dealers	Trading Venues	Central Counterparties	Central depositories	Trade repositories	Payment systems	Participants	Fund management companies	SICAV	Limited partnerships for CIS	SICAF	Custodian banks	Managers domestic CIS	Distributors	Representatives of foreign CISs	Other intermediaries	SROs	DSFIs	SRO Supervised	Audit firms	Rating Agencies
X	X						X																				

Table of Content

I. Topic

This Circular substantiates Articles 89-94 of the Capital Adequacy Ordinance (CAO; SR 952.03) and sets out 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 sets out how to determine the capital requirements for operational risks 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 Risks. 1*

II. Definition

According to Article 89 CAO, operational risks are defined as "the threat of losses, resulting from the inadequacy or failure of internal processes, people or systems or as a consequence of external events". This definition shall comprise all legal and compliance risks insofar as these represent a direct financial loss, i.e. including regulatory fines imposed by regulatory authorities and out-of-court settlements. 2*

Repealed 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

where

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

- α shall always be set at 15%; 6

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

- 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 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

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*

[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.

B. The Standard 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 βi 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 Standard Approach K_{SA} shall be calculated as follows: 25

where

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

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

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

Repealed 28*

In accordance with Annex 1, every bank must define 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 Standard 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 Management must be familiar with the basic concept of the approach and be in a position to exercise its corresponding oversight function. 53*

Banks must have an operational risk management system that is conceptually sound, reliable and is 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 risks; 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 quantification system must be an integral part of the monitoring and controlling of 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 capital for operational risks to major business lines and for creating incentives to improve the management of operational risks 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], FINMA does not specify a certain approach but instead leaves banks considerable freedom in this regard. This circular shall therefore be limited to setting out the key requirements that mandatorily 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 FINMA and shall 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 shall 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 the definition of operational risk which is compatible with the defnition set out in Article 89 CAO and margin no. 2. In addition, they must also allow a categorization of loss events in accordance with Annex 2. 71*

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 of incorporating the following: 74

- internal loss data (margin nos. 76–85);

[3] Cf. footnote 1

- relevant external loss data (margin nos. 86–88);
- scenario analysis techniques (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)

Banks 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 shall also define who is authorized to make such alterations and up to what degree. 76

Banks must use an internal loss database. Upon first using 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 Annex 2. It shall maintain documented and objective criteria for this categorization. 79*
- The bank's internal loss data must be captured comprehensively through a robust and adequate 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 gross minimum amount. This gross minimum amount is defined by the FINMA. 80
- For each loss event, the bank shall 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 of the loss event must also be documented. 81
- Banks 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 be included in the internal operational risk loss database if 83

they are 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.

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 be integrated into the institution-specific approach. Banks 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

Building on expert opinion in conjunction with external data, scenario analyses 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 bank's current 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 shall 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 shall 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 of 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 be recognized only if the insurer cedes the risk exposure to an independent third-party entity (e.g. a reinsurer) that in turn 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 is permitted to limit the use of an institution-specific approach to individual areas of activity, and cover remaining areas with the Basic Indicator Approach or the Standard Approach, provided that the following conditions are 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

- Banks must have a timeline for the rollout of their institution-specific approach across all of their material legal entities and business lines. 111

- It is not permitted to retain the Basic Indicator or Standard 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 Standard 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 permitted to use different approaches to determine capital requirements for operational risks. 114

E. Adjustment to Capital Requirements (Article 45 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 impose themselves in particular if a determination of capital requirements exclusively based on the Basic Indicator or Standard 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 risks according to the institution-specific approach, 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 theoretically have had if it had applied the Basel I minimum standard[5]. In application of Article 47 CAO, the FINMA stipulates for each institution how it may calculate an adequate approximation of the theoretical Basel I requirements. For operational risks, it shall refer to the Standard Approach as described in Article 93 CAO. 116*

IV. Qualitative requirements on handling operational risk

A. Principle of Proportionality

While the requirements and duties described in this chapter shall in principle apply to all addressees of this circular, they may vary depending on the relevant institution's size, complexity, structure and risk profile. Margin no. 119 lists the margin numbers from which requirements small institutions shall be exempted. 117*

Banks and securities dealers in FINMA categories[6] 4 and 5 shall be deemed to be small institutions as per margin no. 117. In individual cases, the FINMA may order the easing or tightening of requirements. 118*

B. Basic Qualitative Requirements

Small institutions as described in margin nos. 117 and 118 shall be exempt from requirements stipulated in margin nos. 129, and 132-134. 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)[7] 120*

a) Principle 1: Categorization and Classification of Operational Risk

In order to ensure the consistency regarding risk identification, risk assessment and the targeting in the operational risk management, operational risks shall be consistently categorized[8]. 121*

The standardized classification of operational risks shall take place based on the categorization of operational risks in accordance with margin no. 121 and shall include an assessment of both the institution's inherent risks[9] and the residual risks[10]. The classification may be prepared either on a qualitative or a quantitative basis. The classification shall in particular also serve to determine the operational risks with far-reaching implications as per margin no. 137. 122*

---

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, **AS 1998** 16).

6 Cf. appendix of the FINMA circ. 11/2 "Capital buffer and capital planning - Banks".

7 www.bis.org/publ/bcbs195.pdf

8 This standardized categorization may be prepared based on Annex 2 of this circular or using an internal terminology or taxonomy.

9 Cf. Annex 3, margin no. 59

10 Cf. Annex 3, margin no. 60

Repealed 123*

Repealed 124*

b) Repealed

Repealed 125*

Repealed 126*

Repealed 127*

c) Principle 2: Identification, Mitigation and Monitoring

An effective risk identification, which forms the basis for the limitation and monitoring of operational risks, shall take into account both internal[11] and external[12] factors. These shall include at least risk and control assessments as well as audit findings. 128*

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

a. collection and analysis of internal loss data;

b. collection and analysis of external events related to 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[13]

The organizational units entrusted with the mitigation and monitoring shall do this by using the instruments, structures, approaches, etc. defined in the conceptual framework for the institution-wide risk management defined in FINMA circular 2017/1 "Corporate Governance". 130*

[11] For example, a bank's corporate structure, type of activities, employee qualifications, organiza-tional changes and staff fluctuations.

[12] For example, changes to the bank's larger environment and the industry as such, as well as tech-nological developments.

[13] 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.

d) Principle 3: Internal and External Reporting

Repealed 131*

An internal reporting on operational risk shall include financial, operational and compliance data as well as significant external risk-relevant 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 required capital for operational risks: 132*

a. significant breaches of the bank's defined risk tolerance for inherent and residual risk as well as exceedances of fixed risk limits for these; 132.1*

b. details on material internal operational risk events and/or losses; 132.2*

c. information about external events which may be relevant for the institution, and potential risks and their potential impact on the institution. 132.3*

Institutions shall dispose of a formal disclosure policy that has been approved by the ultimate supervision body, setting out how the bank is to disclose its operational risks and which control processes are to be applied with regard to the disclosure. 133*

The data disclosed externally by the institutions must allow stakeholders to obtain an understanding of the bank's approach regarding the management of operational risks. Among other things, this includes a management concept for operational risks, which shall enables stakeholders to assess the effectiveness of the identification, mitigation and monitoring of operational risks. 134*

e) Principle 4: Technological Infrastructure[14]

Executive Management shall document in an appropriate manner the management of risks arising from the technology infrastructure, in accordance with the institution's IT strategy and its defined risk appetite as well as taking into consideration aspects relevant to the institution in accordance with internationally recognized standards. 135*

Executive Management shall ensure that the management of technology infrastructure risks covers at least the following aspects: 135.1*

a. Current overview regarding the most significant components of the network infrastructure and an inventory of all critical applications and IT infrastructure related thereto, as well as interfaces with third parties; 135.2*

b. Explicit definition of roles, duties and responsibilities regarding critical applications as well as IT infrastructure related thereto and critical and/or sensitive data and processes; 135.3*

c. A systematic process to identify and assess IT risks in the course of a due diligence review, particularly in cases of acquisitions or outsourcings relating to IT services, and with regard to 135.4*

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

monitoring service provider agreements;

d. Processes to enhance employee awareness regarding their responsibility to mitigate IT risks and adhere to and reinforce requirements on IT information security: 135.5*

Moreover, Executive Management shall document the management of cyber risk[15] in an appropriate manner. This concept shall at least cover the following aspects and shall ensure an effective implementation with the help of appropriate processes as well as an explicit definition of tasks, roles and responsibilities: 135.6*

a. Identification of potential institution-specific threats resulting from cyber-attacks[16], in particular with regard to critical and/or sensitive data and IT systems; 135.7*

b. Protection of business processes and of technology infrastructure from cyber-attacks, in particular with regard to the confidentiality, the integrity and availability of critical and/or sensitive data and IT systems; 135.8*

c. Timely recognition and recording of cyber-attacks on the basis of processes used for the systematic monitoring of technology infrastructure; 135.9*

d. Reaction to cyber-attacks with timely and targeted measures and, in case of significant cyber-attacks that threaten the continuation of normal business activities, in coordination with the BCM, and 135.10*

e. Ensuring timely restoration of normal business activities after a cyber-attack through appropriate measures. 135.11*

Executive Management shall have vulnerability tests[17] and penetration tests[18] performed regularly in order to protect critical and/or sensitive data and IT systems against cyber-attacks. These must be performed by qualified staff with adequate resources. 135.12*

f) Principle 5: Continuity in the event of a business interruption

Executive Management must dispose of business continuity plans for the institution which ensure the continuity of activities and limitation of damage in the event of a serious business interruption[19]. 136

g) Principle 6: Continuity of Critical Services in the Event of Liquidation and Restructuring of Systemically Important Banks

Systemically important banks shall define relevant measures in their contingency plans which would allow a uninterrupted continuation of systemically important functions (Article 9(2)(d) BA in conjunction with 136.1*

[15] Operational risks with regard to potential losses due to cyber-attacks.
[16] These are attacks from the Internet and similar networks on the integrity, availability and confidentiality of technology infrastructure, specifically in regard to critical and/or sensitive data and IT systems.
[17] Analysis used to identify current software weaknesses and security gaps in the IT infrastructure causing vulnerability towards cyber-attacks.
[18] Focused review of software weaknesses and security gaps in the technology infrastructure that could be exploited as entry-points for unauthorized access to said technology infrastructure.
[19] Cf. FINMA circular 2008/10 "Self-regulation as a minimum standard" for items in the recognized minimum standards of the SBA recommendations for Business Continuity Management (BCM).

Articles 60 et seqq. BO). They shall identify the necessary services critical for the continuation of systemically relevant functions in the case of a liquidation, a reorganization or restructuring of the bank ("critical services") and take the measures necessary to continue these services. In doing so, they shall take into consideration regulations issued by international standard setters in this regard.

h) Principle 7: Risks Arising from Crossborder Services

If institutions or their group entities provide financial services or distribute financial products across borders, the risks resulting from the application of foreign laws (tax laws, criminal laws, money laundering laws, etc.) shall be adequately recorded, mitigated and monitored. As the regulatory authority, the FINMA in particular expects institutions to adhere to the foreign supervisory laws. 136.2*

Institutions shall perform in-depth analyses of the legal frameworks and the related risks with regard to their cross-border financial service business and their cross-border distribution of financial products. Based on these analyses, institutions shall undertake the necessary strategic and governance measures to eliminate and mitigate the risks and adapt these measures regularly in case of changing conditions. In particular they shall dispose of the necessary country-specific expertise, define the specific service provision models for the countries in question, train their employees and ensure the adherence to the guidelines with organizational measures, directives as well as remuneration and sanction models. 136.3*

Moreover, risks generated by external asset managers, brokers and other service providers shall also be taken into consideration. Therefore, an institution shall act prudently in the selection and instruction of these partners. 136.4*

This principle applies also to constellations where subsidiaries domiciled abroad, branch offices or similar units of a Swiss financial institution provide cross-border services to clients. 136.5*

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 FINMA circular 13/3 "Auditing" and capture the findings of their audit procedures in the audit report. 139*

Annex 1

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

I. Overview

1

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 transactions, 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, lending, guarantees and sureties, exchange business
Payment and settlement operations[20]	External clients	Payment transactions, clearing and securities settlements for third parties

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

1st Level	2nd Level	Activities
Custodial and fiduciary transactions	Custody	Escrow, deposit business, custody, securities lending for clients; similar services for companies
	Trust business	Issuers and paying agents
	Corporate trusts	
Institutional asset management	Discretionary asset management	Pooled, segmented, retail, institutional, closed, open, private equity
	Non-discretionary asset management	Pooled, segregated by segment, retail, 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 All banking or non-banking activities which are not directly linked to the bank's core business activities, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports. 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, an objective mapping criteria must be used. 3

3 If an activity cannot be mapped to a particular business line based on objective criteria then it has to 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 the above must be clearly identified and substantiated. 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

Annex 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 intended to defraud, misappropriate property or circumvent regulations, the law or company policies (involving at least one internal party)	Unauthorized activities	Transactions intentionally not reported Unauthorized transactions causing monetary losses Intentionally entering positions erroneously
		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 intended to defraud, misappropriate property or circumvent regulations, the law or company policies (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)

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
Workplace	Losses arising due to infringements of labor, security or health laws and regulations, including all compensation payments	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	Damages arising from all types of discrimination
Clients, products & business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation towards specific clients, or from the nature or design of a product	Duties of suitability, disclosure & safe custody	Breaches of safe-custody duty, violations of guidelines Issues in regard to suitability or disclosure (know-your-customer rules, etc.) Violation of information requirements Violation of banking secrecy and/or data protection provisions Aggressive sales practices Inappropriate generation of commissions and brokerage fees Misuse of confidential information Lender liability

Loss Event Category (Level 1)	Definition	Sub-Categories (Level 2)	Examples of activities (Level 3)
		Improper business or market practices	Breach of antitrust provisions Improper 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 & 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 system failures	Technical systems	Hardware Software Telecommunication Power failures, etc.

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 mandatory 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
		Business partners	Faulty service from a business partner (non-client) Various disputes with business partners (non-client)
		Vendor and suppliers	Outsourcing Disputes with vendors and suppliers

Annex 3*

Handling of Electronic Client Data

This annex shall set out the principles and explanations on the proper management of risks related to the confidentiality of electronic personal data of natural persons ("private clients"[21]) whose customer relations are 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[22], but also in data protection law[23] and in civil law. 1*

Small banks[24] shall be exempt from complying with the following margin nos.: 2*

- Margin nos. 15, 17-19 and 22 of Principle 3;
- All margin nos. of Principles 4-6;
- Margin no. 41 of Principle 7.

Concerning the implementation of the requirements of Annex 3, institutions pursuant to Article 47a–47e CAO and institutions pursuant Article 1b BA may limit themselves to margin no. 3. In individual cases, the implementation of margin number 3 shall depend on the size, the complexity, the structure and risk profile of the institution. 2.1*

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. The Board of Directors shall supervise Executive Management in order to ensure an effective implementation of measures to secure the confidentiality of client data. Executive Management shall mandate an independent unit to exercise a control function with the task of creating a 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*

[21] "Private clients" shall also include business relationships where a natural person enters a busi-ness 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.

[22] In particular Articles 3 and 47 BA as well as Article 12 BO; Articles 10 and 43 SESTA and Articles 19 et seq. SESTO.

[23] In particular Article 7 DPA and Article 8 et seqq. OFADP (cf. also FDPIC guidelines ; available at www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de).

[24] Cf. margin no. 118.

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

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 shall take into account the bank's size and complexity. It must be consistently implemented by all functions and units that are processing or have access to client data. 6*

The measures and the periodicity of their implementation must be specified in writing and in a comprehensible and binding manner, on the basis of the 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 ensured through regular controls carried out 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 potential 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 13*

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.

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 (DPA). Special controls are required for physical locations (e.g. server rooms) or network zones that store or allow access to large quantities of CID. Data access must be clearly defined and may be granted only on a strict "need-to-know" basis. 15*

a) Data storage location and access in general

An inventory must be available and kept up-to-date showing the applications and the corresponding infrastructure that contain or process CID. In particular, this inventory must be updated in a timely manner in case of structural changes (e.g. new locations or a renewal of the technical infrastructure). Changes having minor consequence must be updated regularly. 16*

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

- where CID is archived, which applications and IT systems process CID and from where CID can be accessed electronically (end-user applications); 18*
- which national and international locations and units can access data (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, increased risks associated with respect to client data protection must be adequately mitigated[25]. 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 rights of employees and third parties. To ensure that only individuals currently autho- 22*

[25] Moreover, the institution must comply with the specific provisions of the data protection legislation, specifically Article 6 DPA.

rized have access to CID, permissions must be reconfirmed regularly.

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 bank's size and the level of complexity of its IT architecture. 24*

b) Security standards and market practice

Security standards form an integral part of the framework ensuring client data confidentiality. They shall 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 be subject to increased security measures. They must be monitored with particular attention. 30*

a) Careful selection of employees

Employees with access to CID must be selected carefully. In particular, potential employees must be scru- 31*

tinized prior to starting their activity to verify whether they fulfill the requirements for adequate handling of CID. The bank must also contractually stipulate how third parties are to select employees and define employees from third parties, who will access CID on the bank's behalf, so that all employees undergo a similarly diligent selection process.

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 define 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[26] to mass CID ("key employees") shall be subject to 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[27] (key employees) and/or have responsibilities with respect to the controlling and monitoring client data confidentiality. 34*

Measures such as keeping log files shall be implemented in order to identify 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 shall identify and evaluate inherent risks and residual risks regarding CID confidentiality using a structured process. This process must comprise risk scenarios[28] relating to 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*

[26] In case of expanded access rights, such as the querying and extraction/migration of mass CID.
[27] Individual queries with limited access rights (e.g. by front office employees) shall not be considered access to mass CID.
[28] Either on 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 based on a description of purely hypothetical, seri-ous incidents.

b) Risk scenarios and key controls[29]

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*

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 where large quantities of CID have to be modified or migrated.[30] 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*

If an institution does not apply methods to anonymize, pseudonymize or encrypt data (i.e. they use the normal data) during the development, change or migration of systems (e.g. when generating test data or in the interim storage of data during a data migration), then it must apply the prescriptions of margin no. 40 to these activities. 41.1*

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

Banks are expected to 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 Executive 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*

---

[29] 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 Prac-tice by the Working Group Information Security of the Swiss Bankers Association" (passed in Oc-tober 2012).

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

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 to ensure the confidentiality of CID (margin no. 6, 7 and 8) and 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*

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 shall continue 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*

b) 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*

c) General responsibility

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

d) 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(a) DPA and make it possible to identify the clients involved. 52*

Mass client-identifying data: 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 from 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 is no longer subject to the DPA.[31] 65*

[31] Cf. FDPIC, Annex to the Guidelines on the Minimum requirements of a Data Protection Management System, 5.

List of amendments

The circular has been amended as follows:

These amendments were passed on 1 June 2012 and shall enter into force on 1 January 2013.

Amended margin no.	84

In addition, the references to the Capital Adequacy Ordinance (CAO; SR 952.03) have been adapted to the version entering into force on 1 January 2013.

These amendments were passed on 29 August 2013 and shall enter into force on 1 January 2014.

Newly inserted margin no.	116

These amendments were passed on 29 August 2013 and shall enter into force on 1 January 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 March 2014 and enter into force on 1 January 2015.

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

These amendments were passed on 22 September 2016 and shall enter into force on 1 July 2017.

Newly inserted margin nos.	132.1-132.3, 135.1-135.12, 136.1-136.5
Amended margin nos.	2, 53, 117, 118, 119, 121, 122, 128, 129, 130, 132, 133, 134, 135, 136, 137
Repealed margin nos.	2.1, 123, 124, 125, 126, 127, 131
Other changes	Chapter IV.B.: new enumeration of principles

These amendments were passed on 31 October 2019 and shall enter into force on 1 January 2020.

Amended margin nos.	122, 135, 135.1, 135.6

The appendices to the circular were amended as follows:

These amendments were passed on 29 August 2013 and shall enter into force on 1 January 2015.

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

New	Appendix 3
Repealed	Appendices 1 and 4

These amendments were passed on 22 September 2016 and shall enter into force on 1 July 2017.

New	Annex 3: margin no. 41.1
Amended	Annex 1: margin no. 9
	Annex 2: Title of annex
	Annex 3: margin nos. 2, 3, 5, 6, 7, 8, 16, 17, 30, 33, 34, 56

These amendments were passed on 31 October 2019 and shall enter into force on 1 January 2020.

New	Annex 3: margin no. 2.1

Contacts

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

Helen Campbell
Partner, Banking Transformation
Tel. +41 58 249 35 01
hcampbell@kpmg.com

Thomas Dorst
Partner, Assurance & Regulation
Tel. + 41 58 249 54 44
tdorst@kpmg.com

Nicolas Moser
Partner, Geneva Office
Tel. +41 58 249 37 87
nmoser@kpmg.com

www.kpmg.ch