KPMG

FINMA Circular 2008/21 (Excerpt)

IT risk management concept
Deal with cyber risk
Handling of electronic client data

dated 22 September 2016

Principle 4: Technological Infrastructure[1]

Executive Management shall implement an IT risk management concept reflecting the institution's IT strategy and its defined risk tolerance that takes into consideration the relevant aspects in accordance with internationally recognized standards. 135*

Executive Management shall ensure that the **IT risk management concept** addresses 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 monitoring service provider agreements; 135.4*

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 implement a risk management concept on how to **deal with cyber risk**[3]. This concept shall at least cover the following aspects and shall ensure an effective implementation through appropriate processes as well as through an explicit definition of tasks, roles and responsibilities: 135.6*

a. Identification of potential institution-specific threats resulting from cyber-attacks[5], 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*

---

[1] 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.

[3] Operational risks with regard to potential losses due to cyber-attacks.

[5] 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.

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

Executive Management shall have vulnerability tests[6] and penetration tests[7] 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*

[6] Analysis used to identify current software weaknesses and security gaps in the IT infrastructure causing vulnerability towards cyber-attacks.

[7] 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.

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"[8]) 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[9], but also in data protection law[10] and in civil law. 1*

Small banks[11] 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.

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*

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*

---

8 "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.

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

10 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).

11 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 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 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*

14*

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

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[12]. 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 authorized have access to CID, permissions must be reconfirmed regularly. 22*

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

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 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*

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

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

h. 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 scrutinized 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 31*

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[13] 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[14] (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[15] 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*

[13] In case of expanded access rights, such as the querying and extraction/migration of mass CID.

[14] Individual queries with limited access rights (e.g. by front office employees) shall not be considered access to mass CID.

[15] 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[16]

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.[17] 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*

---

[16] 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).

[17] This usually happens in case of the development, change or migration of systems due to technol-ogy 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*

Contacts

Matthias Bossardt
Partner
Cyber Security
Tel. +41 58 249 36 98
mbossardt@kpmg.com

Roman Haltinner
Director
Cyber Security Services
Tel. +41 58 249 42 56
rhaltinner@kpmg.com

www.kpmg.ch