KPMG

New FINMA circular 2018/03 Outsourcing – Banks and Insurers

Focus on banks and securities dealers

kpmg.ch

Requirements and duties for banks and securities dealers

On 5 December 2017, FINMA published the new circular 2018/03 "Outsourcing – banks and insurers". It will enter into force as at 1 April 2018. Institutions are given a transitional period of five years to adjust their existing outsourcing relationships accordingly. This may cause considerable headaches as managing operational risk will become quite complex.

Focus

The central idea of the revised circular is to make regulations increasingly principle-based and technology-neutral. In all of this, institutions are given more individual responsibility. As such, banks and securities dealers should align their outsourcing relationships better with their business model and its specific risks. Institutions will have to be accountable for specific outsourcing relationships with high risks.

Requirements

FINMA requirements and duties concerning the outsourcing of important functions have increased significantly. The circular mainly focuses on a comprehensive framework that includes the monitoring of all outsourced functions. It foresees more duties in regard to the selection, instruction and control of the service providers, as well as the documentation and the taking inventory of outsourced tasks. This framework is expected to map the financial service provider's risk appetite, which has to be defined beforehand.

The efforts required to implement the new requirements as well as the contractual amendments should not be taken lightly. Moreover, the new requirements pertaining to the in-sourcing of a formerly outsourced task can be quite complex and may also affect other outsourcing relationships. To add to all of this, institutions must now also address group-internal outsourcing relationships that were left unregulated in previous circulars (e.g. security requirements).

Scope of application

The circular applies to banks and securities dealers domiciled in Switzerland as well as branch offices of foreign banks and securities traders. The regulatory standards of the new circular are applicable not only to third-party service providers but also to group-internal outsourcing relationships. Theoretically, group-internal service providers may benefit from a less stringent regime for certain companies but, in practice, the implementation of such alleviations will be anything but easy.

Quick health check: Should you be worried?

- ☐ Could the increased requirements made of outsourcing relationships mean that some processes may benefit from digitalization (for instance, by using robotics)?
- ☐ Have you set up internal policies enabling decision-making in regard to outsourcing projects? If yes, do these meet the requirements of the circular?
- ☐ Have you prepared a concept to re-integrate outsourced functions, and do you dispose of a contingency plan that allows you to carry out the outsourced services in case of an emergency?
- ☐ When selecting a service provider, have you also considered the professional qualifications, and the financial and human resources, besides the concentration risk and the possible consequences of a transfer to a different provider?
- ☐ Do you dispose of a complete and up-to-date list of all agreements with internal and external service providers and their sub-contractors, which serves as a basis to determine whether they constitute an outsourcing as defined in the circular?
- ☐ Do you have outsourced activities that you do not consider to be a significant outsourcing of functions in the sense of FINMA circular 18/03?
- ☐ Are your outsourcing relationships sufficiently documented in the contracts? Do you have full and unhindered access to inspect and review the service provider at all times?
- ☐ Have you defined appropriate risk control measures? Do you monitor the service provider yourself or do you receive adequate confirmations from elsewhere? If you perform your own controls, have these been integrated into your ICS?
- ☐ Have you analyzed the circular's impact if you provide services to other group companies?
- ☐ During the transitional period, how do you handle control reports (e.g. ISAE) that still refer to the former requirements?
- ☐ How will you guarantee an adequate monitoring of these controls?

Actions you need to take based on the circular

We can support you in the analysis of the impact that the new provisions will have on your business and will help you implement these efficiently.

Requirements for banks and securities dealers

Strategic aspects, processes and governance

A **framework for outsourcing relationships** should include the following points:

- Institution-specific definition of **significant/insignificant outsourcing relationships** in consideration of risks and the institution's business model using a decision tree.
- **List of criteria** for the **risk analysis** of the outsourcing relationships at stand-alone level as well as across the entire group in consideration of concentration risks and the risk of dependence on certain service providers.
- **Instructions** on the internal duty to document and evaluate the outsourcing relationship (list of criteria and risk analysis) with defined minimum requirements.
- **Control ownership and continuous monitoring** of outsourcing relationships.
- Creation of an internal position to **monitor and control** the service provider.
- **Contingency plan** with **security requirements** specifically tailored to the institution and the cases on hand **(including group-internal outsourcing).**
- Process to **inventorize significant outsourcing** relationships and document all other outsourcing relationships.
- Definition of **minimum requirements** regarding the **inventorization** (including the definition of data that has to be obtained from the service providers).
- Process on the **orderly re-integration** of outsourcing relationships.

Possible KPMG support

- Establish a **gap analysis** of pending requirements and duties.
- Make available a **framework** (including policies and processes) that enables a holistic management specific to the institution.
- Draw up a **decision tree** on how to define **significant/insignificant outsourcing relationships.**
- **Re-document** outsourcing relationships to ensure their conformity with the more stringent requirements and **draw up an inventory.**
- **Draw up or rework policies** and **processes** to implement and **make available templates of key documents** (e.g. support in the amendment of outsourcing contracts).
- Support in the **amendment of control reports** (ISAE 3402/3000) to reflect the new framework (including inherent controls).
- Define **KPIs** and **limits** regarding the fulfillment of regulatory requirements that need to be monitored centrally.
- Support the **adjustment** of **outsourcing contracts.**

Data and IT

The revised circular is meant to be technology-neutral. For instance, this means that despite the fact that it no longer contains specifics on data protection and business secrecy, these private-law regulations remain applicable. Specifically, this also applies to Annex 3 of FINMA circ. 2008/21 regarding electronic client data, i.e. data that is stored in virtual private servers or in clouds. Consideration should be given to the fact that financial institutions can leverage certain synergies with other regulations when implementing the new circular (example: implementing the new EU General Data Protection Regulation as well as the revised Swiss Data Protection Act). For banks and securities dealers, the following questions and needs arise:

- Rules on how to handle **client-identifying data.**
- Unhindered and uninterrupted availability and readability of data to guarantee a possible **reorganization or unwinding** of an institution.

Possible KPMG support

- Draw up and revise **processes** and **policies** on how **to handle client-identifying data.**
- Provide **IT advice** on **infrastructure, data security** and **data availability** (e.g.: data mirroring).
- **Implement adequate measures** related to the required **access rights** with foreign service providers.
- Create a **risk analysis** during the implementation of the **conceptual framework.**
- **Support the outsourcing of services** (e.g. to a cloud) during the project monitoring, an ongoing risk analysis, the coordination with the service provider and service agreements, etc.

Strategic aspects, processes and governance

The circular enters into force on 1 April 2018. Banks and securities dealers should consider the following aspects:

- The circular's provisions apply immediately to **outsourcing** relationships that have been **concluded** or **amended after 1 April 2018.**
- **Already existing** outsourcing relationships have to be adjusted to meet the new requirements of the circular within the transitional period of **five years.** This transitional period is quite long to allow for the regulating of external factors (e.g. notice periods for contracts) in complex external outsourcing relationships.

Possible KPMG support

- **Set up** or **revise new policies** and **processes** in application of the new rules (definition based on the activities' significance and risk level).
- **Prioritizing** and **planning** of the **implementation**:
  - Prioritizing the outsourcing relationships based on the required actions and supervision efforts
  - Contacting service providers delivering critical services
  - Exchange with service providers
  - Negotiations
  - Implementation plans

Our added value for you:

- Tools ready to go for your agreements.
- Benchmarking
- Efficient project setup enabled by our industry expertise and experience in the area of outsourcing for financial service providers.
- A highly motivated team: Our innovative solutions will bring new impulses and will help make your project a success.

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

Marianne Müller
Partner
FS Assurance & Accounting

+41 58 249 36 76
mariannemueller@kpmg.com

Alex Cejka
Director
FS Technology

+41 58 249 46 47
acejka@kpmg.com

Thomas Bolliger
Partner
Information Governance & Compliance
+41 58 249 28 13
tbolliger@kpmg.com

Prafull Sharma
Partner
Digital Transformation

+41 58 249 77 91
prafullsharma@kpmg.com

kpmg.ch