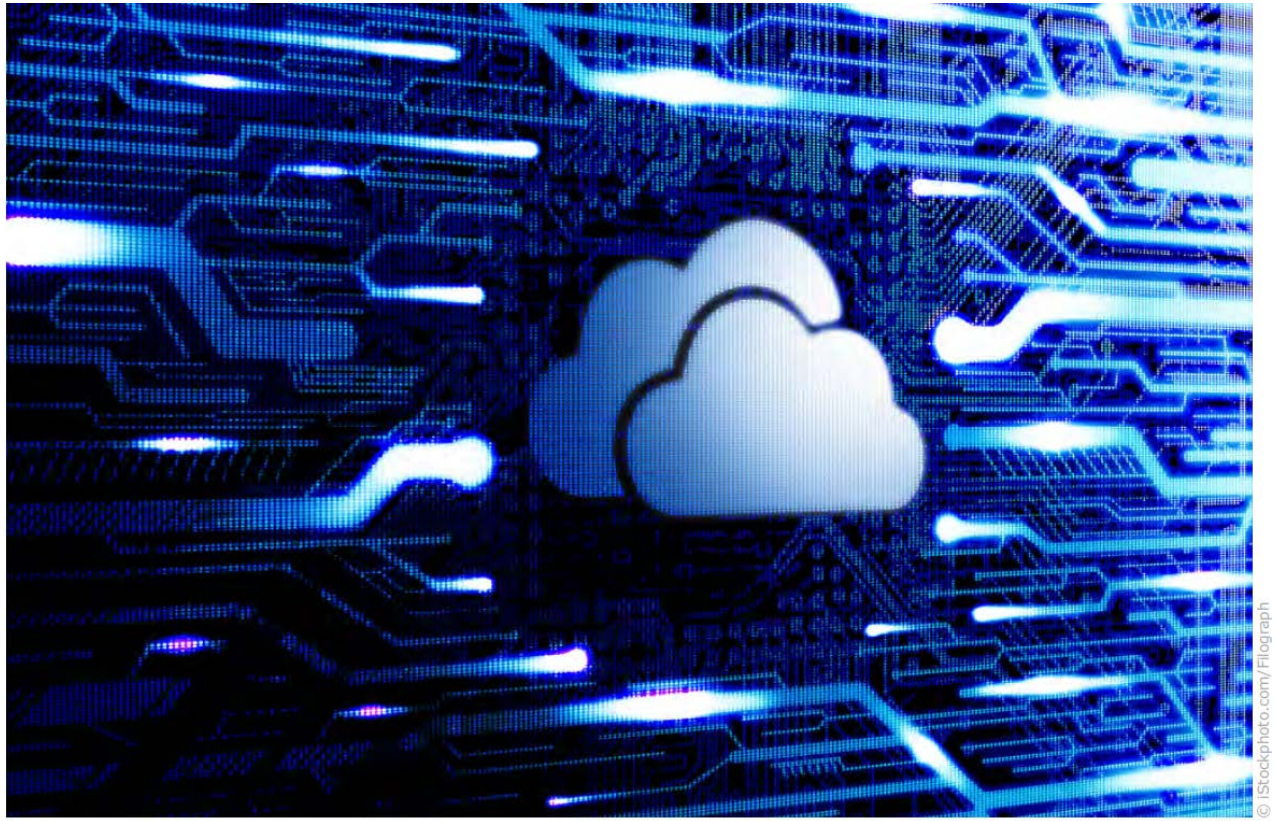
BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht



© iStockphoto.com/Filograph

Grafik Quelle: BaFinJournal

EBA workshop: Recommendations on Cloud Outsourcing– Implementation in Germany

Renate Essler,
BaFin

Supervisory Approach for Cloud Outsourcing in Germany

- Legal Framework for Outsourcing in Germany
- EBA Recommendation on Outsourcing to Cloud Service Providers
- EBA Draft Guidelines on Outsourcing arrangements
- BaFin plans to publish a supervisory manual with respect to cloud outsourcing

Supervisory Experience – Assessment of the Cloud Service Provider

- The use of cloud services must be **assessed** in advance. If this assessment reveals that, in terms of risk, the planned outsourcing constitutes as material, then the institutions must comply with sections 25a and 25b of the German Banking Act in conjunction with AT 9 number 7 and 8 of the Minimum Requirements for Risk Management (including Outsourcing) for the contractual arrangements.
- Minimum Requirements for Risk Management also apply to the use of cloud services where this constitutes outsourcing of IT services (Supervisory Requirements for IT in Financial Institutions including IT Outsourcing, BaFin circular from 2017).
- Institutions must comply with the supervisory requirements for outsourcing pursuant to sections 25a and 25b of the German Banking Act in conjunction with AT 9 of the Minimum Requirements for Risk Management to the extent necessary in each **individual case**.

Supervisory Experiences – Contractual rights

- The outsourcing contract must ensure BaFin's unrestricted rights of information and audit and **ability to monitor** in relation to the outsourced activities and processes.
- BaFin's ability to monitor the cloud service providers must be the same as its ability to supervise the supervised entities as provided for by law. This includes, in particular, the option to perform **on-site inspections**.
- The rights of information and audit of the **internal audit function** of the outsourcing institution must be granted in full through the outsourcing contract.
- The outsourcing institution must have the opportunity to influence the **scope** of the information and audit.

Supervisory Experiences – Restriction of contractual rights

- **Phased information** and audit procedures constitute such a restriction and do not comply with the requirements of the MaRisk or the EBA Recommendations on Outsourcing to Cloud Service Providers.
- If performing the audit is made dependent on the concept of **commercial reasonableness**, then this is also generally regarded as a restriction.
- Contractual obligation to **first rely** on standardised audit reports made available by the cloud service providers also constitutes an impermissible restriction of the rights of information and audit.
- If an institution decides **not to perform** the audit itself or not to perform the audit alone, this must not result in a restriction of the institution's right of audit.

Supervisory Experiences – Certifications

- Institutions may use certificates based on **common standards** (eg., ISO 270xxx, C 5 requirements catalog of the Federal Office for Information Security), audit reports of recognized third parties or internal audit reports of the cloud service provider.
- Institutions should **not rely** on certificates alone and should take hereby into account the scope, depth, timeliness and suitability of the certifier or auditor of these certificates and audit reports.
- As Internal Audit uses such certificates or audit reports in the course of its work, it should be able to examine the **underlying evidences**.

Supervisory Experiences – Simplification

- Institution's audits may be performed also by the internal audit function of the cloud service provider. In this case, the **internal audit findings** of the cloud service provider must be passed on to the internal audit function of the outsourcing institution.
- BaFin accepts **pooled audits** in order to render audits more efficient both ways for institutions and also for the cloud service providers.
- Pooled audits may be performed by the **internal audit function** of the outsourcing institutions or by a third party commissioned by these insitutions.

Collaborative Cloud Audit Group

- Foundation in 2017 (around 10 members)
- open format to conduct Cloud Audits in a collaborative format
- accessible to all regulated financial institutions
- audits are performed by a subset of the group and announced open upfront to allow all interested institutions to join
- first on-site mission of a cloud service provider by the Collaborative Cloud Audit Group in 2018

Contact

Renate Essler

Federal Financial Supervisory Authority (BaFin)

Tel. +49 (0)228 / 4108-2440

renate.essler@bafin.de

Banking Supervision, Group IT Supervision