BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Guidance on outsourcing to cloud service providers

Banking Supervision
Division: Policy Issues relating to IT Supervision and Inspections

Last updated: November 2018

Contents

I. Preliminary remarks

The subject of outsourcing to cloud service providers in the financial sector has become increasingly relevantt in recent years. As a result, BaFin and the Deutsche Bundesbank over the past months have been in discussions with supervised companies about plans for outsourcing to cloud service providers. At the same time, the German supervisory authorities have also entered into a dialogue with different cloud service providers. One focus of these discussions has been on the terms of the (standard) contracts or supplementary contractual agreements which are to meet and stipulate the relevant requirements under supervisory law, e.g. information and audit rights of both the supervised companies and the supervisory authorities.

This subject has also caught the attention of the European supervisors. At the EIOPA and EBA level, within the SSM, as well as bilaterally between the national supervisory authorities, a constant exchange about how to deal with outsourcing to cloud service providers has now emerged. The most recent outcome of this is the Recommendations on Outsourcing to Cloud Service Providers of the EBA (EBA/REC 2017/03) from December 2017.

With this Guidance, BaFin and the Deutsche Bundesbank give their joint assessment on outsourcing to cloud service providers. That said, this Guidance does not establish any new requirements but instead reflects the current supervisory practice in such outsourcing cases, and in particular is intended to create greater transparency as regards the supervisory assessment on various passages in contract clauses. But since not all (standard) contracts or contractual supplementary agreements are known to the German supervisory authorities, this Guidance does not make any claim to completeness.

Furthermore, the Guidance in particular pursues the objective of creating for the supervised companies an awareness of the issues involved in dealing with cloud services and the related requirements of supervisory law. In this regard the Guidance draws attention to various aspects that the supervised companies should take into account when outsourcing to cloud service providers, e.g. in the context of risk analysis and contractual terms; it is not, however, exhaustive.

The Guidance is addressed to those companies supervised in the financial sector (credit institutions, financial services institutions, insurance undertakings, pension funds, investment services enterprises, asset management companies, payment institutions and e-money institutions). The following statements therefore have to be read in the context of the supervisory law requirements applicable in each case.

Supervisory law requirements for outsourcing remain unaffected. An outsourcing may not result in the responsibility of managers of the supervised company for the items outsourced being transferred to the cloud service provider. The supervised company continues to be responsible for compliance with the statutory provisions to be observed by the supervised companies.

II. Explanatory notes

The term "**outsourcing**" is used in this Guidance for "outsourcing" within the meaning of section 25b of the German Banking Act (*Kreditwesengesetz* – KWG), section 80 of the German Securities Trading Act (*Wertpapierhandelsgesetz* – WpHG), section 26 of the German Payment Services Oversight Act (*Zahlungsdiensteaufsichtsgesetz* – ZAG) and section 36 of the German Investment Code (*Kapitalanlagegesetzbuch* – KAGB), as well as for "outsourcing" within the meaning of Article 274 Commission Delegated Regulation (EU) 2015/35 and section 32 of the German Insurance Supervisory Act (*Versicherungsaufsichtsgesetz* – VAG) .

The term "**material**" is used in the following for the terms "important/critical" within the meaning of Article 274 Commission Delegated Regulation (EU) 2015/35 and section 32 VAG as well as for the term "essential" within the meaning of section 25b KWG and section 26 ZAG.

The term "**items**" is used collectively for the "activities and processes" within the meaning of section 25b KWG, section 26 ZAG or for "important functions/insurance activities" within the meaning of Article 274 Commission Delegated Regulation (EU) 2015/35 and section 32 VAG, as well as for "tasks" within the meaning of section 36 KAGB.

Cloud services are services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

As a rule, cloud services are provided as

- Infrastructure as a Service (**IaaS**, provision of computing power and memory space),
- Platform as a Service (**PaaS**, provision of development platforms) or
- Software as a Service **(SaaS,** provision of software applications/ web applications)

(service models).

The service models differ in terms of the user's organisational and/or technical control options. In the case of IaaS, the user has full control over the IT system from the operating system upwards (i.e. the provider always has control over the physical environment), since everything is operated within their sphere of responsibility. In the case of PaaS, the user only has control over their applications that run on the platform, and in case of SaaS the user practically hands over the entire control to the cloud service provider.[2] The more complex the service model is, the lower the user's control options in the cloud are. However, a loss of control possibilities is not synonymous with a loss of responsibility under supervisory law.

[1] EBA/REC/2017/03 of 20 December 2017, page 3.

[2] Cf. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (last accessed on 26 October 2018).

In practice, a further distinction may be made by four deployment models for cloud services:

- **Private cloud:** Cloud infrastructure available for exclusive use by a single company.
- **Community cloud:** Cloud infrastructure available for exclusive use by a specific community of companies, including several companies of a single group.
- **Public Cloud:** Cloud infrastructure available for open use by the general public.
- **Hybrid cloud:** Cloud infrastructure made up of two or more distinct cloud infrastructures.[3]

The following statements are to be considered independent of the selected service or deployment model.

III. Strategic considerations

When developing its IT strategy, the supervised company is to include aspects on the use of cloud services. In addition, a supervised company should develop and document a process covering all steps of relevance for outsourcing to the cloud service provider, from the strategy, migration to the cloud, right through to the exit strategy. It is important for the supervised company to first review all relevant internal processes to determine whether these are ready for "the cloud" before it goes ahead with such outsourcing. In this context particularly risk management and control processes of the supervised company must be considered in addition to the items to be outsourced.

IV. Analysis and materiality assessment

Following the strategic decision to outsource items to a cloud service provider, the first thing the supervised company should do in the process is review on an individual case basis the respective requirements of supervisory law to determine whether a case of outsourcing exists and whether it is to be qualified as material. As a rule, a case of outsourcing has to be assumed.

The risk analysis is to take account of all aspects that are relevant for the supervised company in connection with outsourcing to cloud service providers, with the extent of the analysis depending on the type, scope, complexity and risk content of the outsourced items. If materiality requirements of supervisory law exist, these must be observed. On the basis of the risk analysis the supervised company should determine on its own responsibility which outsourcings are material with regard to risks.

In the **risk analysis**, the following points as a rule should be considered:

- the content of the cloud service used,

[3] EBA/REC/2017/03 of 20 December 2017, page 3.

- the critical nature of the item to be outsourced, i.e. an assessment of whether the item is critical for the continuation of the supervised company's business operations,
- an assessment of the risks arising from the selected service as well as deployment model,
- an assessment of the financial risks, operational risks (e.g. system failure, sabotage), including the legal risks (e.g. risks of legal enforcement, risks of data protection law) as well as reputational risks; these also include considerations regarding data storage and data processing locations,
- an assessment of the suitability of the cloud service provider (capabilities, infrastructure, financial situation, corporate law and regulatory status, etc.); to the extent sensible, supporting documentation/certificates may be used on the basis of common standards (e.g. international security standard ISO/IEC 2700X of the International Organization for Standardization, Cloud Computing Compliance Controls Catalogue (C 5 Catalogue) of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI)), audit reports of recognised third parties or internal audit reports fo the cloud service provider,
- an assessment of the risks in the case of several items being outsourced to a cloud service provider,
- an assessment of the risks involving oversight limitations in those countries where the items are performed or the data are stored or processed,
- an assessment of the geopolitical situation (wider political and security stability) and the applicable law (including data protection laws) in the jurisdictions in question, the law enforcement provisions in place in those jurisdictions, including the insolvency law provisions that would apply in the event of a cloud service provider's failure,
- an assessment of the risks to the integrity, availability, confidentiality and authenticity of the items, as well as the processed or stored data, taking account of
    - any possible means of access to data by other jurisdictions,
    - risks from different interfaces between own and external systems,
    - risks resulting from extraordinary contract termination such as loss of data, restrictions on transferability of the data to a new service provider,
- assessment of the risks arising from chain-outsourcing by the cloud service provider.

In the event of material defects becoming known as well as material changes in the cloud service to be provided by the cloud service provider, it has to be kept in mind that this may have impacts on the risk situation of the outsourcing and thus on the outsourcing company. Accordingly, the risk analysis should at least be reviewed or repeated.

V. Contractual terms in the case of (material) outsourcing

Depending on the supervisory law requirements, the following terms and conditions in particular should be included in the outsourcing agreement for material outsourcing or for non-differentiated outsourcing according to the KAGB:

1. Scope of performance

The agreement should include a specification, and if necessary a description, of the service to be performed by the cloud service provider. This should be stipulated in what is referred to as the service level agreement. In this context, the following aspects should be defined:

- the item to be outsourced and its implementation (e.g. type of service and deployment model, scope of services offered such as computing power or available memory space, availability requirements, response times),
- support services,
- responsibilities, duties of cooperation and provision (e.g. in the case of updates),
- place of performance (e.g. location of data centres),
- commencement and end of outsourcing agreement,
- key ratios for performing ongoing review of service level,
- indicators for identifying an unacceptable service level.

2. Information and audit rights of supervised company

Information and audit rights as well as control possibilities of the supervised company must not be subject to contractual restrictions. It has to be ensured that the supervised company receives the information it needs to adequately control and monitor the risks associated with the outsourcing.

To safeguard the information and audit rights, the following terms in particular should be contractually agreed:

- grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the related processes and controls,
- the possibility of performing on-site audits of the cloud service provider (and where applicable of the chain-outsourcing company),
- effective possibilities of controlling and auditing the entire outsourcing chain.

No (indirect) restriction of rights

Effective exercise of the information and audit rights may not be restricted by contract. The German supervisory authorities consider such impermissible restriction of information and auditing rights to exist particularly in the case of contractual agreements granting such rights only subject to certain conditions.

This particularly includes:

- agreeing on incremental information and audit procedures, e.g. the obligation to first rely on the audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider before the supervised company can perform its own auditing activities,
- restricting performance of information and audit rights to submission of audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider,
- linking information access to prior attendance of special training programmes,
- wording a clause in such a way that performance of an audit is made conditional on its commercial reasonableness,
- limiting the performance of audits in terms of timing and personnel; as a general rule, however, it is acceptable to limit access to customary business hours upon advance notice,
- making reference to exclusive use e.g. of management consoles for exercising information and audit rights of the company,

- specifying the procedure as well as the scope by which information and audit rights are exercised by the cloud service provider.

Exemptions

Depending on the applicable requirements under supervisory law, the supervised companies may claim exemptions to make their own audit activities more efficient. Such exemptions are pooled audits or the use of documentation/certificates based on common standards or of audit reports of recognised third parties or of internal audit reports of the cloud service provider.

Pooled audits

Supervised companies subject to compliance with sections 25a, 25b KWG may avail themselves of exemptions in Circular 09/2017 (BA) – Minimum Requirements for Risk Management – (MaRisk). Pursuant to BT 2.1 Item 3 MaRisk, the internal auditing function of the supervised company in the case of material outsourcing may forego own auditing activities provided that the auditing work carried out by the external service provider meets the requirements of AT 4.4 and BT 2 MaRisk. The internal auditing function of the supervised outsourcing company must satisfy itself at regular intervals that these conditions are met. The audit findings concerning the supervised company are to be passed on to the internal auditing function of the supervised outsourcing company.

In this regard the auditing activity may be performed by the internal audit department of the cloud service provider, the internal audit department of one or more of the supervised outsourcing companies on behalf of the supervised outsourcing companies ("pooled audits"), a third party appointed by the cloud service provider or a third party appointed by the supervised outsourcing companies.

For the other supervised companies, it may be permissible in the individual case to exercise certain information and audit rights against the cloud service provider jointly with other supervised companies by way of pooled audit.

If a supervised company avails itself of one of the aforementioned exemptions, this may not result in its information and audit rights being restricted.

Proof/certificates and audit reports

The supervised company as a general rule may use documentation/certificates on the basis of common standards (e.g. international security standard ISO/IEC 2700X of the International Organization for Standardization, Cloud Computing Compliance Controls Catalogue (C 5 Catalogue) of the BSI), audit reports of recognised third parties or internal audit reports of the cloud service provider. The supervised company in this regard must take account of the scope, depth of detail, up-to-dateness and suitability of the certifier or auditor of such documentation/certificates and audit reports.

However, a supervised company must not rely solely on these when exercising its audit activity. Where the internal audit department uses such documentation/certificates in its activity, it should be able to examine the evidence underlying them.

3. Information and audit rights of supervisory authorities

Information and audit rights as well as control possibilities of the supervisory authorities must not be subject to contractual restrictions. The supervisory authorities must be able to monitor cloud service providers exactly as the applicable law provides for the supervised company. It must be possible for the supervisory authorities to exercise their information and audit rights as well as control possibilities properly, and without restriction, as regards the item being outsourced; this also applies to those persons whom the supervisory authorities use when performing the audits.

To safeguard these rights, the following terms in particular should be contractually agreed:

- obligation of the cloud service provider to cooperate with the supervisory authorities without restriction,
- grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the processes and controls relating thereto as well as the possibility of performing on-site audits of the cloud service provider (and where applicable of the chain-outsourcing company),
- effective possibilities of controlling and auditing the entire outsourcing chain.

No (indirect) restriction of rights

Such impermissible restriction of information and auditing rights as well as control possibilities of the German supervisory authorities is deemed to exist particularly in the case of provisions granting such rights only on certain conditions. We refer to the above statements on the restriction of the rights of the supervised companies to avoid repetition.

4. Rights to issue instructions

Rights of the supervised companies to issue instructions are to be agreed. The rights to issue instructions are to ensure that all required instructions needed to perform the agreed service can be issued, i.e. the possibility of influencing and controlling the outsourced item is required. The technical implementation may be organised individually based on the company's specific circumstances.

If the supervised company uses proof/certifications or audit reports (cf. V.2), it should also have the possibility of influencing the scope of proof/certifications or audit reports so that it can be expanded to include relevant systems and controls. There should be a reasonable proportion in how many and how often such instructions are issued.

Moreover, the supervised company should be authorised at all times to issue instructions to the cloud service provider for correction, deletion and blocking of data and the cloud service provider should be allowed to collect, process and use the data only in the context of the instructions issued by the supervised company. This should also cover the possibility of issuing an instruction at any time to have the data processed by the cloud service provider transferred back to the supervised company promptly and without restriction.

If the explicit agreement on the rights of the supervised company to issue instructions can be waived, the service to be provided by the outsourcing company is to be specified with sufficient clarity in the outsourcing agreement.

5. Data security/protection (reference to location of data storage)

Provisions ensuring compliance with data protection regulations and other security requirements are to be agreed.

The location of data storage must be known to the supervised company. This should include the specific location of the data centres. As a general rule, giving the name of the location (e.g. the town or city) will suffice for this purpose. However, if the supervised company should need the precise address of the data centre based on considerations of risk management, the cloud service provider should provide it.

Moreover, redundancy of the data and systems should be ensured so that in the event of a failure of one data centre it is ensured that the services are maintained.

The security of the data and systems is also to be ensured within the outsourcing chain.

The supervised company must have the possibility of quickly accessing at all times its data stored with the cloud service provider and of re-transferring the same if required. In this regard it has to be ensured that the selected form of re-transfer does not restrict or exclude the use of the data. For that reason, platform-independent standard data formats should be agreed. Compatibility of the different system must be taken into account.

6. Termination provisions

Termination rights and adequate termination notice periods are to be agreed. In particular, a special termination right, providing for termination for good cause if the supervisory authority calls for the agreement to be ended, should be agreed.

It has to be ensured that in the event of termination the items outsourced to the cloud service provider continue to be provided until such time that the outsourced item has been completely transferred to another cloud service provider or to the supervised company. In this regard it has to be guaranteed in particular that the cloud service provider will reasonably assist the supervised company in transferring the outsourced items to another cloud service provider or directly to the supervised company.

The type, form and quality of transfer of the outsourced item and the data should be defined. If data formats are adapted to the individual needs of the supervised company, the cloud service provider should deliver a documentation of such adaptations on termination.

It should be agreed that after re-transfer of the data to the supervised company its data have been completely and irrevocably deleted on the side of the cloud service provider.

To ensure that the outsourced areas are maintained in the event of the planned or unplanned termination of the agreement, the supervised company must have an exit strategy and review its feasibility.

7. Chain outsourcing

Provisions on the possibility and the modalities of chain-outsourcing ensuring that the requirements of supervisory law continue to be met are to be agreed. Restrictions resulting, e.g., in only the most substantially similar obligations being assumed are not permissible. It must be ensured in particular that the information and audit rights as well as controlling possibilities of the supervised outsourcing company as well as of the supervisory authorities also apply to subcontractors in the case of chain-outsourcing.

With a view to chain-outsourcing, reservations of consent of the outsourcing company or specific conditions to be met in order for chain-outsourcing to be possible should be provided for in the outsourcing agreement. It should be defined which outsourced items and/or portions thereof may be chain-outsourced and which ones may not.

The supervised company should be informed in advance of chain-outsourcing of the outsourced items and/or portions thereof in text form. The subcontractors and the items and/or portions thereof chain-outsourced to them should be known to the supervised company.

In the event of a new chain-outsourcing, it has to be kept in mind that this may have impacts on the risk situation of the outsourcing and thus on the outsourcing company. Accordingly, the risk analysis should at least be reviewed or repeated in the event of a new chain-outsourcing. This also applies where material defects as well as material changes in the cloud service provided by subcontractors become known.

The company should review and monitor the performance of the entire service on an ongoing basis, regardless of whether the cloud service is provided by the cloud service provider or its subcontractors.

8. Information duties

Provisions are to be agreed ensuring that the cloud service provider informs the supervised company about developments that might adversely affect the orderly performance of the outsourced items. That includes things like reporting any disruptions in providing the cloud service. This is to ensure that the company can adequately monitor the outsourced item.

The cloud provider is to inform the supervised company without delay about any circumstances that might pose a risk to the security of the supervised company's data to be processed by the cloud service provider, e.g. as a result of acts by third parties (e.g. attachment or confiscation), insolvency or composition proceedings, or other events.

It should be ensured that the supervised company is adequately informed by the cloud service provider in advance in the event of relevant changes in the cloud service to be provided by the cloud service provider. Service descriptions and any changes to them should be provided and/or notified to the supervised company in text form. It should be ensured that the supervised company is adequately informed, to the extent permitted by law, where any requests/demands for surrender of data of the supervised company are made by third parties.

9. Notice of applicable law

Where a choice of law clause is agreed and German law is not agreed as the governing law, the law of a country from the European Union or the European Economic Area should at any event be agreed as the law governing the agreement.