OVERVIEW

No. RADAR
4243

Responsible level
EU

Competent authority
ESMA – European Securities and Markets Authority

Standard designation
Guidelines for outsourcing to cloud providers

Title of Standard
Guidelines on outsourcing to cloud service providers

Abbreviation (standard)

Short Title

Abbreviation (standard)
ESMA50-164-4285

Abbreviation
ESMA50-164-4285

Implementation status of the standard
published

Industry relevance
Banking industry

category
02. Capital Markets Law

Document type
Guideline

Management Summary
Against the backdrop of increasing outsourcing to cloud providers, ESMA is publishing these guidelines to create consistent, efficient, and effective supervisory practices within the European System of Financial Supervision (ESFS). The guidelines are based on the analysis of the response to the EU FinTech Action Plan (COM(2018) 109 final) and the subsequent engagement with stakeholders. Due to the cross-sectoral use of cloud
Outsourcing and the similarity of the main risks associated with it, the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02, Dataset 3141)* as well as the *EBA*

Recommendations on outsourcing to cloud providers (EBA/REC/2017/03, dataset 2414) and the *EIOPA Guidelines on Cloud Outsourcing (EIOPA-BoS-20-002, Dataset 3706)* were taken into account in the preparation of these guidelines. As a form of IT outsourcing, cloud outsourcing is subject to the general principles and requirements for outsourcing. However, certain characteristics are specific to cloud services, which tend to be more standardized than more traditional forms of IT outsourcing and are provided to the outsourcing companies in a highly automated and large-scale manner. These guidelines support companies and competent authorities in identifying, addressing, and monitoring risks and challenges arising from outsourcing agreements with cloud providers. Aspects ranging from the decision to outsource, the selection of a cloud provider, and the monitoring of outsourced activities to the consideration of exit strategies are addressed. The nine guidelines cover the following topics:

- Governance, control and documentation;
- Outsourcing risk analysis and due diligence review;
- Central elements of the contract;
- Information security,
- Exit strategies;
- Right of access and inspection;
- Sub-outsourcing;
- Written notification to the competent authorities and
- Monitoring outsourcing agreements with cloud providers.

Management Summary

In the context of increasing outsourcing to cloud providers, ESMA publishes these guidelines to establish consistent, efficient and effective supervisory practices within the European System of Financial Supervision (ESFS). The guidelines are based on the analysis of the responses to the EU FinTech Action Plan (COM(2018) 109 final) and the subsequent exchange with firms and stakeholders. Considering that the main risks associated with cloud outsourcing are similar across sectors, ESMA take into account the recent guidelines published by EBA and EIOPA, namely the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02, Dataset 3141)*, which have incorporated the *EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03, data set 2414)*, and the *EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002, data set 3706)* in the preparation of these guidelines. As a form of IT outsourcing, outsourcing in the cloud is subject to the general principles and requirements for outsourcing. Nevertheless, certain features are specific to cloud services which tend to be more standardized than more traditional forms of IT outsourcing and are provided in a highly automated manner and at large scale. These guidelines will help firms and competent authorities to identify, address and monitor risks and challenges arising from cloud outsourcing arrangements. They address aspects ranging from the decision to outsource, the selection of a cloud service provider, the monitoring of outsourced activities to the provision of exit strategies. The nine guidelines cover the following topics:

- governance, oversight and documentation;
- pre-outsourcing analysis and due diligence;

- contractual requirements;
- information security;
- exit strategies;
- access and audit rights;
- sub-outsourcing;
- written notification to competent authorities and
- Supervision of cloud outsourcing arrangements.

CONTENTS

Main content

These guidelines contain a wide range of provisions that affect outsourcing in general. In addition to the core statements, only those provisions that are specifically relevant to outsourcing to cloud providers are described below.

Guidelines on outsourcing to cloud providers (Annex III)

1. Guideline 1: Governance, Control and Documentation

A company should have an up-to-date cloud outsourcing strategy that is consistent with other relevant strategies, internal policies and processes, such as those related to information and communication technology, information security and operational risk management.

Among other things, companies should consider proportionality aspects (see source for details)

- Clearly assign responsibilities for the documentation, management and control of cloud outsourcing agreements;
- allocate sufficient resources to comply with these guidelines and the legal requirements relevant to cloud outsourcing;
- set up a function to monitor outsourcing.

Small and less complex companies should at least ensure a clear separation of management and control of outsourcing arrangements. Companies should reassess whether an outsourcing arrangement is critical and material at regular intervals and when there are significant changes to the outsourced function. Companies should create an outsourcing register that identifies critical and material outsourcing. The minimum scope of this register, as specified in these guidelines, includes, for example, cloud deployment models and the type of data and locations (see source for details). For arrangements that concern non-critical or non-material functions, the information to be included in the register should be determined in relation to the outsourced function.

2. Guideline 2: Outsourcing risk analysis and due diligence review

Before concluding outsourcing agreements with cloud providers, the outsourcing company should check whether critical or essential functions are affected, all relevant risks

evaluate, conduct appropriate due diligence on the cloud service provider (CSP) and identify and assess potential conflicts of interest.
The analysis and due diligence review should be proportionate to the nature, scope, and complexity of the outsourced function and the resulting risks (proportionality aspect). At a minimum, an assessment of the potential impact of the outsourcing agreement with cloud providers on operational risks, as well as legal, compliance, and reputational risks, should be conducted. For the outsourcing of critical or essential functions, additional risks must also be assessed, which may arise from the following issues, for example (see source for details):

- the migration and implementation processes;
- the compatibility of systems and applications;
- the portability of data;
- political stability and applicable legal system (e.g. insolvency law, data protection regulations, including the question of whether the conditions for data transfer to third countries are in accordance with *Regulation (EU) 2016/679, GDPR, dataset 641*, are given)
- the concentration on a few providers.

A review and, if necessary, a repeat of the due diligence must be carried out if the agreements are to be changed or if significant deficiencies or changes in the service provided become known.

3. Guideline 3: Key elements of the contract
The rights and obligations of the outsourcing company and the CSP should be clearly assigned and set out in writing.
When outsourcing critical or essential functions, contracts should include certain minimum requirements. These include, for example, the regions or countries in which the outsourced function operates and where data storage takes place, conditions for relocation, the provision of reports to the security officer, and the recovery of data (see source for details).

4. Guideline 4: Information security
Companies should establish proportionate information security requirements in their internal policies and procedures, as well as in cloud outsourcing contracts, and continuously monitor compliance with these requirements (including the protection of confidential, personal, or other sensitive data).

When outsourcing critical or essential functions, the following aspects must be considered on a risk-based basis, without prejudice to the GDPR requirements (see source for details):
- Organization of information security;
- Identity and access management;
- Encryption and key management;
- Operational and network security;
- Application programming interfaces;
- Business continuity and disaster recovery;
- Data location and

- Compliance with and monitoring of international information security standards.

5. Guideline 5: Exit strategies

When outsourcing critical or essential functions, the company should ensure that the outsourcing can be terminated at any time without unnecessary disruption to business operations or services, in compliance with applicable legal requirements and the confidentiality, integrity and availability of its data.
To this end, exit and transition plans must be developed and alternative solutions identified. Furthermore, it must be ensured that, upon termination of the outsourcing, the outsourced activities and all related data are fully transferred to the company or another service provider and, if necessary, removed from the previous service provider's systems (see source for details). When developing the exit strategy and alternative solutions, the following factors, for example, must be considered (see source for details):

- Indicators of exit-triggering events;
- Identification of required resources through impact analysis;
- Conducting risk-based adequacy assessments;
- Determining criteria for a successful transition.

6. Guideline 6: Right of access and review

The written agreement on cloud outsourcing must not restrict the effective exercise of the company's access and audit rights or its supervisory capabilities.
If exercising these rights results in risks for the CSP or its customers, alternatives should be agreed upon that ensure a comparable outcome. Companies may, if necessary, rely on third-party certifications and external or internal audit reports. However, for critical or essential outsourcing, they should aim to reduce their long-term dependence on third-party certifications or audit reports to meet legal requirements. When outsourcing critical or essential functions, certain minimum requirements must be met when using third-party certifications or audit reports, such as (see source for details):

- the permanent integration of the systems and central controls and compliance with legal requirements by the CSP;
- the regular assessment of the scope and content;
- the sufficient competence of the auditors;
- the right to carry out on-site inspections.

Since cloud outsourcing is a technically complex topic, external or internal auditors must have the appropriate skills and knowledge (see source for details).

7. Guideline 7: Sub-outsourcing

If sub-outsourcing of critical or essential functions is (partially) permitted, the written outsourcing agreement between the company and the CSP should be (details see source)

- Define parts or aspects of the function that are excluded from sub-outsourcing;
- specify the conditions for sub-outsourcing;
- define that the CSP monitors the further outsourced services;

- ensure that the intention to sub-outsource is communicated to the company in good time to allow a risk analysis;

- ensure a right of objection or consent from the company.

8. Guideline 8: Written notification to the competent authorities
The planned outsourcing of critical or essential functions should be reported to the competent authority promptly. The minimum information that must be reported in writing, taking into account the principle of proportionality, includes various details on the outsourced function, the contractual agreements, and the cloud service provider, as well as information on the cloud provisioning model, including storage locations and the type of data, as well as any sub-outsourcing (see source for details). The criticality or materiality classification must be justified.

9. Guideline 9: Monitoring outsourcing agreements with cloud providers In particular, cloud outsourcing agreements relating to the outsourcing of critical or essential functions must be assessed by the competent authorities with regard to the resulting risks. It must be ensured that effective supervision can be carried out even if critical or essential functions are performed outside the EU.

Based on a risk-based approach, competent authorities must assess whether companies' governance structures, resources, and processes are adequate and effective, and whether companies are able to identify and address relevant risks appropriately. In the case of concentration risks, competent authorities should monitor their development and assess potential impacts (see source for details).

CATEGORIZATION

Keywords

Notification obligation, outsourcing, cloud outsourcing, exit strategy, cyber risk, cloud provider, CSP, cloud service provider, data availability, data protection, service, service provider, disaster recovery, due diligence, exit strategy, IT system, IT outsourcing, information security, concentration risk, emergency plan, recovery, outsourcing, outsourcing agreement, key function, monitoring measure, confidential information, confidentiality, risk analysis, essential outsourcing, sub-outsourcing, materiality, critical outsourcing, right of access, right of audit, third countries, GDPR

Legal and information bases

- Guidelines on Cloud Outsourcing (EIOPA-BoS-20-002) (Dataset 3706)
- Guidelines on outsourcing arrangements (EBA/GL/2019/02) (Dataset 3141)
- Recommendations on outsourcing to cloud providers (EBA/REC/2017/03) (Dataset 2414)
- Regulation (EU) 2016/679 (GDPR) (Dataset 641)
- FinTech Action Plan (COM(2018) 109 final)

Related Standards

- Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002) (data record 3706)
- Guidelines on outsourcing arrangements (EBA/GL/2019/02) (Dataset 3141)
- Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03) (data record 2414)
- Regulation (EU) 2016/679 (GDPR) (Dataset 641)
- FinTech Action Plan (COM(2018) 109 final)

Target group – credit institutions
Yes

Target group – financial services institutions
Yes

Target group – Other companies in the financial sector
Yes

Target group – payment institutions
No

Target group – insurance companies
No

Target group – supplement
The guidelines apply to competent authorities as well as to (a) alternative investment fund managers (AIFMs) and depositaries of alternative investment funds (AIFs), (b) undertakings for collective investment in transferable securities (UCITS), management companies and depositaries of UCITS, and Investment firms that have not appointed a management company, c) central counterparties (CCPs), including Tier 2 CCPs from third countries that comply with the relevant EMIR requirements, d) trade repositories (TRs), e) investment firms and credit institutions when carrying out investment services and activities, data transmission service providers and market operators of trading venues, f) central securities depositories (CSDs), g) credit rating agencies (CRAs), h) securitisation repositories (SRs) and i) administrators of critical benchmarks.

Comments
These apply to competent authorities and to a) alternative investment fund managers (AIFMs) and depositaries of alternative investment funds (AIFs), b) undertakings for collective investment in transferable securities (UCITS) management companies and depositaries of UCITS as well as investment companies that have not designated a management company, c) central counterparties (CCPs), including Tier 2 third-country CCPs which comply with the relevant EMIR requirements, d) trade repositories (TRs), e) investment firms and credit institutions when carrying out investment services and activities, data reporting services providers and market operators of trading venues, (vi) central securities depositories (CSDs), f) credit rating agencies (CRAs), g) securitization repositories (SRs), and h) administrators of benchmarks and administrators of critical benchmarks.

Statement by (date)

Implementation status Explanation

Status – Further Details

Date of entry into force/publication

May 10, 2021

Entry into force estimated?

No

Date of first application

31.07.2021

Application appreciated?

No

Date Standard repealed

Remark (Entry into force/Publication)

The guidelines apply to all cloud outsourcing agreements entered into, renewed, or amended from July 31, 2021. Organizations should ensure that existing outsourcing agreements comply with the requirements of these guidelines by December 31, 2022. If the review of cloud outsourcing agreements for critical or essential functions is not completed by December 31, 2022,

Within two months of the publication of the Guidelines in all official EU languages (publication on 10 May 2021), competent authorities will inform ESMA whether they comply with the Guidelines, do not comply but intend to do so, or do not comply with the Guidelines and do not intend to do so (comply-or-explain procedure).

Publication of the compliance table on 24 November 2021 (update: 28 January 2022):
Germany/BaFin: applies the guidelines;
Austria/FMA: applies the guidelines;
Luxembourg/CSSF: applies the guidelines;
SSM/ECB: not applicable.

Comments

The guidelines apply from July 31, 2021 to all cloud outsourcing arrangements entered into, renewed or amended on or after this date. Firms should ensure that existing cloud outsourcing arrangements comply with these guidelines by December 31, 2022. Where the review of cloud outsourcing arrangements of critical or important functions is not finalized by December 31, 2022.

Within two months of the date of publication of the guidelines on ESMA's website in all EU official languages (publication on 10 May 2021), competent authorities must notify ESMA whether they comply, do not comply, but intend to comply, or do not comply and do not intend to comply with the Guidelines (comply-or-explain procedure).

Publication of the compliance table on November 24, 2021 (update: January 28, 2022):
Germany/BaFin: complies with the guidelines;
Austria/FMA: complies with the guidelines;

Luxembourg/CSSF: complies with the guidelines;
SSM/ECB: not applicable.

Sources

The sources are not shown in this working paper.