Cloud Compliance Center - France

Rules for cloud outsourcing

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes. In France, the French banking supervisor (Autorité de Contrôle Prudentiel et de Résolution ("**ACPR**")) makes and supervises the rules on outsourcing that apply to credit institutions, payment services providers and investment services providers. The rules are found in the Order of 3 November 2014 on internal control measures (Articles 231-240). However, these provisions do not apply to branches of foreign institutions that must comply with the provisions of their home state regulator. That being said, if they are EU member states, the European Banking Authority ("**EBA**") guidelines on outsourcing arrangements dated 25 February 2019 will still apply (see below).

There are further rules on outsourcing relevant to alternative investment funds (Article 318-58 to Article 318-61) and UCITS (Article 321-93 to Article 321-96) fund managers in the rulebook of the French financial markets supervisor (Autorité des Marchés Financiers).

There are rules on outsourcing for insurers in Articles L. 354-3 and R. 354-7 of the Insurance Code, complemented by Article 274 of the Delegated Regulation No. 2015/35 and an instruction of the ACPR No. 2019-I-06 of 15 March 2019.

Reference should also be made generally to the EBA guidelines on outsourcing arrangements and applicable from 30 September 2019 to credit institutions, payment services providers (payment institutions and e-money providers), as well as to financial services providers subject to the EU Capital Requirements Directive.

With the exception of the EBA guidelines, these rules are mandatory in nature; in practice, however, the EBA guidelines are also regarded as binding. In this regard, the French supervisor has notified the EBA of its intention to respect the guidelines.

**Critical and important functions**

Even though the rules on outsourcing are scattered in different legal texts and depend on the nature of the obliged entity and the competent regulator, they all have one point in common: a distinction needs to be made between the outsourcing of critical and important functions and other types of outsourcing. If an institution outsources critical or important functions, the requirements are stricter compared to the outsourcing of non-important or nonessential functions. Critical or essential functions are defined differently depending on the applicable text. In summary, any function that is the essence of the regulated service to be delivered and those that would have a serious impact on the business if their performance were to cease are deemed critical or important functions.

Any service that covers critical or important functions can only be outsourced to an entity that is authorized to carry on such services according to its national law.

Obliged entities that outsource critical or important functions remain liable toward the regulator. It is not acceptable for outsourcing to transform an obliged entity into a letterbox. In particular, obliged entities must ensure the following:

Outsourcing does not entail any delegation of responsibility of the directors

Outsourcing does not change the relationship between the obliged entity and its customers or the obligations of the entity toward the customers

Outsourcing should not alter the conditions of the license of the obliged entity

The obliged entity must be able to control and manage the risks related to the outsourced activity

Any outsourced function must be covered by internal control measures (permanent, periodic, etc.) of the obliged entity. The obliged entity must take into account the measures put in place by the cloud service provider, which must be chosen with care. The obliged entity must ensure that confidential information is treated as such by the cloud service provider.

The obliged entity must put in place an outsourcing policy. It must ensure that the cloud service provider is able to fulfill its duties and comply with all relevant laws and regulations. The obliged entity must be prepared to act in cases where the cloud service provider is not able to fulfill its duties any longer so that any interruption does not have an adverse effect on services to clients. The obliged entity must ensure that contingency planning is in place.

The cloud service provider may not unilaterally change the service. It must comply with the obliged entity's procedures and must enable the obliged entity to access information. The cloud service provider must inform the obliged entity of any relevant information, particularly information that might affect its ability to continue providing the services. It must further provide the supervisory authority or any foreign competent supervisory authority with access to information and documents and accept on-site inspections.

The EBA guidelines specifically address IT and cloud outsourcing at page 37 and onwards. They require that the cloud service provider be able to appropriately protect the confidentiality, integrity and availability of data. Sub-outsourcing is also addressed whereby the conditions for subcontracting should be clear. Finally, it is provided that the obliged entity must be able to terminate the agreement if any adverse matters are identified as part of a risk assessment. In case of the sub-outsourcing of important or critical functions, the obliged entity must be notified beforehand of any termination.

More generally, the EBA guidelines require that an outsourcing entity do the following:

Put sound governance arrangements in place.

Appropriately manage third-party risk.

Put in place an outsourcing policy.

Manage conflicts of interest related to outsourcing.

Put in place a business continuity plan.

Ensure that the internal audit function covers the outsourcing arrangements.

Ensure the outsourcing arrangements are documented.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.