Deloitte.

**Deloitte Note:**
EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)

# Table of Contents

Outsourcing is a way to get relatively easy access to new technologies and to achieve economies of scale.

# 1 High-Level summary of the issued Guidelines

## 1.1 Executive summary

Financial institutions have been increasingly interested in outsourcing business activities in order to reduce costs and improve their flexibility and efficiency. In the context of digitalisation and the increasing importance of new financial technology (fintech) providers, financial institutions are adapting their business models to embrace such technologies. Outsourcing is a way to get relatively easy access to new technologies and to achieve economies of scale.

The responsibility of the institutions' management body for the institution and all its activities can never be outsourced. Outsourcing is also relevant in the context of gaining or maintaining access to the EU's financial market.

Critical Functions from a resolution perspective may also be outsourced but outsourcing arrangements should not create impediments to the resolvability of the institution. Institutions should be able to effectively control and challenge the quality and performance of outsourced functions and be able to carry out their own risk assessment and ongoing monitoring.

Competent authorities are required to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system. To identify such risk concentrations, competent authorities should be able to rely on comprehensive documentation on outsourcing arrangements compiled by financial institutions.

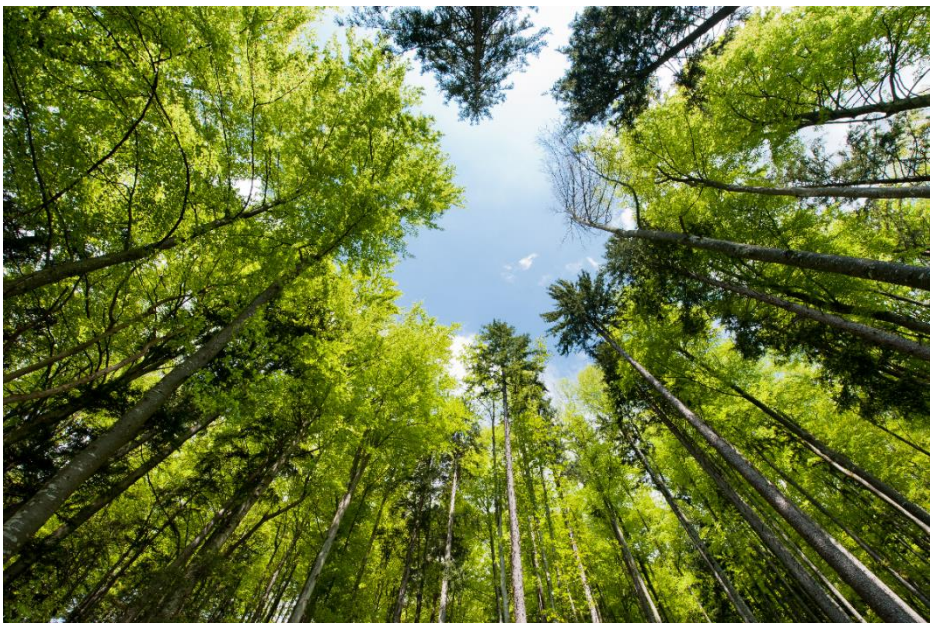
Directive 2013/36/EU (Capital Requirements Directive; CRD) strengthens the governance requirements for institutions and Article 74(3) CRD gives the EBA the mandate to develop guidelines on institutions' governance arrangements. Outsourcing is one of the specific aspects of institutions' governance arrangements. Directive 2014/65/EU (Markets in Financial Instruments Directive; MiFID II) contains explicit provisions regarding the outsourcing of functions in the field of investment services and activities. Directive 2015/2366/EU (Revised Payment Service Directive; PSD2) sets out requirements for the outsourcing of functions by payment institutions.

In order to make it even easier for competent authorities to effectively supervise outsourcing arrangements, the EBA has updated the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing; the aim is to establish a more harmonised framework for all financial institutions that are within the scope of the EBA's mandate, namely credit institutions and investment firms subject to the CRD, as well as payment and electronic money institutions.

The guidelines include requirements that aim to ensure:

a. effective day-to-day management and oversight by the management body;
b. a sound outsourcing policy and processes that reflect the institution's strategy and risk profile;
c. effective and efficient internal control framework;
d. proper identification of critical or important functions and suitability of potential service providers;
e. that all the risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, reported and, as appropriate, mitigated;
f. protection of customer data across the whole institution, including the outsourced functions;
g. appropriate plans for the exit from outsourcing arrangements of critical or important functions, e.g. by migrating to another service provider or by reintegrating the critical or important outsourced functions; and
h. competent authorities remain able to effectively supervise institutions.

The guidelines will enter into force on 30 September 2019, with the 2006 guidelines on outsourcing being repealed at the same time.



## 1.2 Background

The guidelines specify the internal governance arrangements, including sound risk management practices, that institutions, payment institutions and electronic money institutions should implement when they outsource functions, in particular with regard to the outsourcing of critical or important functions.

The guidelines also specify how the arrangements should be reviewed and monitored by competent authorities, by fulfilling their duty to monitor the continuous compliance of entities to which these guidelines are addressed with the conditions of their authorisation.

Institutions should comply with these guidelines on a solo basis, sub-consolidated basis and consolidated basis. The application on a solo basis

might be waived by competent authorities. Payment institutions and Electronic money institutions should comply with these guidelines on an individual basis. Competent authorities responsible for the supervision of institutions, payment institutions and electronic money institutions should comply with these guidelines.

### 1.2.1 Compliance and reporting obligations

Competent authorities must notify the EBA that they comply or intend to comply with these guidelines, or otherwise give reasons for non-compliance. In the absence of any notification by the deadline, competent authorities will be considered by the EBA to be non-compliant. Any change in the status of compliance must also be reported to the EBA. Notifications will be published on the EBA website.

### 1.2.2 Timings

These guidelines apply from 30 September 2019 to all outsourcing arrangements entered into, reviewed or amended on or after this date. For existing outsourcing arrangements institutions should review these with a view to ensuring that these are compliant with these guidelines.

Where the review of outsourcing arrangements of critical or important functions is not finalised by 31 December 2021, institutions should inform their competent authority of that fact, including the measures planned to complete the review or the possible exit strategy.

Institutions should complete the documentation of all existing outsourcing arrangements, other than for outsourcing arrangements to cloud service providers, in line with these guidelines following the first renewal date of each existing outsourcing arrangement, but by no later than 31 December 2021.

The Committee of European Banking Supervisors (CEBS) guidelines on outsourcing of 14 December 2006 and the EBA recommendations on outsourcing to cloud service providers are repealed with effect from 30 September 2019.

# 2 Guidelines on outsourcing

## 2.1 Guidelines 1&2 - Proportionality: groups and institutional protection schemes

The guidelines should apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation. The EU parent undertakings should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and adequate for the effective application of these guidelines at all relevant levels.

Institutions within groups using centrally provided governance arrangements should ensure among others that:

- group management retains full responsibility of compliance;
- outsourcing of operational tasks is effectively performed, monitored and audited;
- management body will be duly informed of relevant planned changes regarding service providers, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels;
- all group institutions should receive a summary of the exit plan for critical or important functions.

Institutions, should also have regard to the principle of proportionality, to ensure that governance arrangements are consistent with:

- the individual risk profile;
- the nature and business model of the institution;
- the scale and complexity of their activities.

Institutions should take into account:

- the complexity of the outsourced functions;
- the risks arising from the outsourcing arrangement;
- the criticality or importance of the outsourced function;
- the potential impact of the outsourcing on the continuity of their activities.

## 2.2 Assessment of outsourcing arrangements

### 2.2.1 Guideline 3 - Outsourcing

Institutions should establish whether an arrangement with a third party falls under the definition of outsourcing. As a general principle, institutions should not consider the following as outsourcing:

a. functions legally required to be performed by a service provider, e.g. statutory audit;
b. market information services;
c. global network infrastructures (e.g. Visa, MasterCard);
d. clearing and settlement arrangements;
e. global financial messaging infrastructures subject to oversight by relevant authorities;
f. correspondent banking services; and

g. the acquisition of services that would otherwise not be undertaken by the institution.

### 2.2.2 Guideline 4 - Critical or important functions

Functions necessary to perform core business activities should be considered as critical or important. When assessing whether an outsourcing arrangement relates to a function that is critical or important, institutions should take into account, a number of factors including:

a. whether a defect or failure in its performance would materially impair their continuing compliance with the conditions or the continuity of their banking and payment services and activities;
b. whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services for which they are authorised;
c. the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:
   - short-and long-term financial resilience and viability;
   - business continuity and operational resilience;
   - recovery and resolution planning, resolvability and operational continuity;
d. the potential impact of the outsourcing arrangement on their ability to:
   - identify, monitor and manage all risks;
   - comply with all legal and regulatory requirements;
   - conduct appropriate audits regarding the outsourced function;
e. the potential impact on the services provided to its clients;
f. the institution's aggregated exposure to the same service provider;
g. the size and complexity of any business area affected.

## 2.3 Governance framework

### 2.3.1 Guideline 5 - Sound governance arrangements and third-party risk

Institutions should have a holistic institution-wide risk management framework extending across all business lines and internal units, identifying, monitoring and managing all their risks, including risks caused by arrangements with third parties.

The risk management framework should also enable institutions to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented across the organisation.

The risk management framework should also cover areas such as cyber risk and compliance with GDPR.

### 2.3.2 Guideline 6 - Sound governance arrangements and outsourcing

The outsourcing of functions cannot result in the delegation of the management body's responsibilities. The management body is at all times fully responsible and accountable for:

a. ensuring that the institution meets on an ongoing basis the conditions with which it must comply to remain authorized;
b. the internal organisation of the institution or the payment institution;
c. the identification, assessment and management of conflicts of interest;
d. the setting of the institution's strategies and policies;
e. overseeing the day-to-day management of the institution, including the management of all risks associated with outsourcing;
f. the oversight role of the management body in its supervisory function;
g. clearly assigning the responsibilities for the documentation, management and control of outsourcing arrangements;
h. the allocation of sufficient resources to ensure compliance with all legal and regulatory requirements;
i. designating a senior staff member who is directly responsible for managing and overseeing the risks of outsourcing arrangements.

### 2.3.3 Guideline 7 - Outsourcing policy

The management body should approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. The policy should include among others:

a. management responsibilities in the decision-making on outsourcing of critical or important functions;
b. the involvement of business lines, internal control functions and other individuals;
c. the planning of outsourcing arrangements;
d. the implementation, monitoring and management of outsourcing arrangements.

The outsourcing policy should differentiate between the following:

a. outsourcing of critical or important functions and other outsourcing arrangements;
b. outsourcing to service providers that are authorised by a competent authority;
c. intragroup outsourcing arrangements and outsourcing to entities outside the group;
d. outsourcing to service providers located within a Member State and third countries.

### 2.3.4 Guideline 8 - Conflicts of interests

Institutions, should identify, assess and manage conflicts of interests with regard to their outsourcing arrangements. Where outsourcing creates material conflicts of interest, including between entities within the same group, institutions need to take appropriate measures to manage those conflicts of interest. When functions are provided by a service provider that is part of the group, the conditions for the outsourced service should be set at arm's length.

### 2.3.5 Guideline 9 - Business continuity plans

Institutions should have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions. Business continuity plan needs to consider that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails.

The institutions need to take into account the potential impact of the insolvency or other failures of service providers and, where relevant, any political risks in the service provider's jurisdiction.

### 2.3.6 Guideline 10 - Internal audit function

The internal audit function's activities should cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and programme should include the outsourcing arrangements of critical or important functions. Internal audit function should at least ascertain:

a. that the institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the management body;
b. the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;
c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the institution's risk strategy;
d. the appropriate involvement of governance bodies; and
e. the appropriate monitoring and management of outsourcing arrangements.

### 2.3.7 Guideline 11 – Documentation requirements

As part of their risk management framework, institutions should maintain an updated register of information on all outsourcing arrangements at the institution and, where applicable, at sub-consolidated and consolidated levels, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.

The register should include at least the following information for all existing outsourcing arrangements:

a. the start date, the next contract renewal date, the end date and/or notice periods for the service provider and for the institution;
b. a brief description of the outsourced function;
c. details of the service provider;
d. the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;
e. whether or not the outsourced function is considered critical or important;
f. in the case of outsourcing to a cloud service provider, the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;
g. the date of the most recent risk assessment and a brief summary of the main results;
h. the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced;
i. identification of alternative service providers.

Institutions should be able to make available to the competent authority either the full register of all existing outsourcing arrangements or sections specified thereof, and should provide this information in a processable electronic form.

Institutions should adequately inform competent authorities in a timely manner about the planned outsourcing of critical or important functions and of any material changes and/or severe events regarding their outsourcing arrangements.

## 2.4 Outsourcing process

### 2.4.1 Guideline 12 - Pre-outsourcing analysis

Before entering into any outsourcing arrangement, institutions should:

a. assess if the outsourcing arrangement concerns a critical or important function;
b. assess if the supervisory conditions for outsourcing are met;
c. identify and assess all of the relevant risks of the outsourcing arrangement;
d. undertake appropriate due diligence on the prospective service provider;
e. identify and assess conflicts of interest that the outsourcing may cause.

#### 2.4.1.1 Guideline 12.1 – Supervisory conditions for outsourcing

Institutions should ensure that the outsourcing of functions of banking activities or payment services, requiring authorisation or registration by a competent authority in the Member State they are authorised, to a service provider in the same or another Member State takes place only if one of the following conditions is met:

a. the service provider is authorised or registered by a competent authority to perform such banking activities or payment services; or
b. the service provider is allowed to carry out those banking activities or payment services in accordance with the relevant national legal framework.

c. With regard to functions outsourced to a service provider located in a third country and for which authorisation or registration by a competent authority in the Member State is required, the conditions are stringent and include:
d. supervision by a relevant competent authority in that third country;
e. appropriate cooperation agreement between the competent authorities responsible for the supervision of the institution; and
f. appropriate access to information, data, documents, premises or personnel of the service provider in the third country that enable the effective application of supervisory tasks.

#### 2.4.1.2 Guideline 12.2 - Risk assessment of outsourcing arrangements

Institutions should consider the expected benefits and costs of the proposed outsourcing arrangement, including weighing any risks that may be reduced/ better managed against any risks that may arise from the proposed outsourcing arrangement.

Institutions should assess the potential impact of outsourcing arrangements on their operational risk, taking into account the assessment on whether the function should be outsourced to a service provider.

Among others, the scenario analysis should include an assessment of:

a. the potential impact of failed or inadequate services;
b. risks caused by processes, systems, people or external events;
c. the principle of proportionality;
d. concentration risk;
e. the aggregated risks resulting from outsourcing several functions;
f. the measures implemented by the institution to manage and mitigate the risks;
g. the risks associated with sub-outsourcing, including additional risks if the sub-contractor is located in a third country/ different country from the service provider;
h. the relevant functions and related data and systems as regards their sensitivity and required security measures.

#### 2.4.1.3 Guideline 12.3 - Due diligence

Institutions should ensure in their selection and assessment process that the service provider is suitable prior to entering into an outsourcing arrangement. Institutions should ensure that the service provider has:

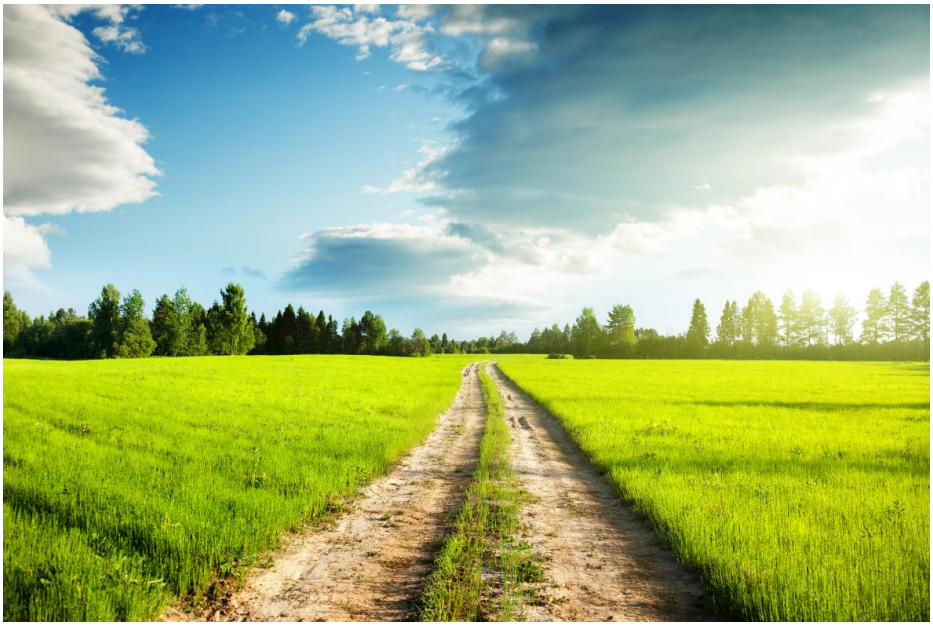
- the business reputation;
- appropriate and sufficient abilities;
- the expertise;
- the capacity and the resources;
- the organisational structure;
- the required regulatory authorisations or registrations to perform the critical or important function;
- the ability to meet its obligations over the duration of the draft contract.

Where outsourcing involves the processing of personal or confidential data, institutions should ensure that the service provider implements appropriate technical and organisational measures to protect the data. Institutions should also take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct.

### 2.4.2 Guideline 13 – Contractual phase

The rights and obligations of the institution and the service provider should be clearly allocated and set out in a written agreement. The outsourcing agreement for critical or important functions should, inter alia, set out:

a. a clear description of the outsourced function to be provided;
b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution;
c. the governing law of the agreement;
d. the parties' financial obligations;
e. the sub-outsourcing conditions, if applicable;
f. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/ or where relevant data will be kept and processed;
g. the right of the institution to monitor the service provider's performance on an ongoing basis;
h. the reporting obligations of the service provider to the institution;
i. the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to the critical or important outsourced function;
j. the termination rights.



#### 2.4.2.1 Guideline 13.1 - Sub-outsourcing of critical or important functions

The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted. Such cases should be recorded in the register. If sub-outsourcing of critical or important functions is permitted, the written agreement should:

a. specify any types of activities that are excluded from sub-outsourcing;
b. specify the conditions to be complied with in the case of sub-outsourcing;
c. specify that the service provider is obliged to oversee those services and ensure that contractual obligations are continuously met;
d. require the service provider to obtain prior specific or general written authorisation from the institution before sub-outsourcing any data;

e. include an obligation of the service provider to inform the institution of any planned sub-outsourcing, or material changes thereof;
f. ensure that the institution has the right to object any intended sub-outsourcing, or material changes, or that explicit approval is required;
g. ensure that the institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing.

#### 2.4.2.2 Guideline 13.2 - Security of data and systems

Institutions should ensure that service providers, where relevant, comply with appropriate IT security standards.

Institutions should define data and system security requirements within the outsourcing agreement and monitor compliance on an ongoing basis. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.

#### 2.4.2.3 Guideline 13.3 - Access, information and audit rights

Institutions should ensure that the outsourcing arrangement prescribes that the internal audit function is able to review the outsourced function using a risk-based approach. The written outsourcing arrangements between institutions and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities with regard to service providers located in a Member State and to service providers located in third countries, ensuring:

a. full access to all relevant business premises including the full range of relevant devices, systems, networks, information and data used ('access and information rights'); and
b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights').

Institutions should also ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.

#### 2.4.2.4 Guideline 13.4 - Termination rights

The outsourcing arrangement should allow the institution to terminate the arrangement, in accordance with applicable law, including in the following situations:

a. where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;
b. where impediments capable of altering the performance of the outsourced function are identified;
c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);
d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and
e. where instructions are given by the institution's competent authority, where it is no longer in a position to effectively supervise the institution.

The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution, thus the outsourcing arrangement should:

a. clearly set out the obligations of the existing service provider in the case of a transfer, including the treatment of data;
b. set an appropriate transition period; and
c. include an obligation of the service provider to support the orderly transfer of the function in the event of the termination.

### 2.4.3 Guideline 14 - Oversight of outsourced functions

Institutions should monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions. The institutions should among others:

- focus on the availability, integrity and security of data and information needs to be ensured;
- material changes on the risk, nature or scale of an outsourced function require reassessment of the criticality or importance of that function by the institution;
- apply due skill, care and diligence when monitoring and managing outsourcing arrangements;
- regularly update their risk and periodically report to the management the risks identified in respect of the outsourcing of critical or important functions;
- monitor and manage their internal concentration risks caused by outsourcing arrangements;
- ensure, on an ongoing basis, that outsourcing arrangements, meet appropriate performance and quality standards in line with their policies;
- take appropriate measures if they identify shortcomings in the provision of the outsourced function.

### 2.4.4 Guideline 15 - Exit strategies

Institutions should have a documented exit strategy when outsourcing critical or important functions that is in line with their outsourcing policy and business continuity plans, taking into account at least the possibility of:

a. the termination of outsourcing arrangements;
b. the failure of the service provider;
c. the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;
d. material risks arising for the appropriate and continuous application of the function.

Institutions should ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities. To achieve this, they should:

a. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested; and
b. identify alternative solutions and develop transition plans to enable the institution to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the institution.

## 2.5 Guidelines on outsourcing addressed to competent authorities

In addition to guidelines addressed to the Institutions, the EBA guidelines include guidelines addressed to the competent authorities.

In particular, competent authorities should aim to identify if outsourcing arrangements amount to a material change to the conditions and obligations of the institutions' initial authorisation.

Competent authorities should be satisfied that they can effectively supervise institutions and ensured that within outsourcing arrangements, service providers are obliged to grant audit and access rights to the competent authority and the institution. Further to the information recorded within the register, competent authorities may ask institutions for additional information for critical or important outsourcing arrangements, such as:

a. the detailed risk analysis;
b. business continuity plan of the service provider, suitable for the services provided to the institution;
c. the exit strategy for use if the outsourcing arrangement is terminated by either party or if there is disruption of the services;
d. the resources and measures in place to adequately monitor the outsourced activities.

Competent authorities may require institutions to provide detailed information on any outsourcing arrangement, even for non-critical/ important functions.

Competent authorities should assess, on a risk-based approach, whether institutions:

a. monitor and manage appropriately critical or important outsourcing arrangements;
b. have sufficient resources in place to monitor and manage outsourcing arrangements;

c. identify and manage all relevant risks;
d. identify, assess and appropriately manage conflicts of interest with regard to outsourcing arrangements, e.g. in the case of intragroup outsourcing;
e. are not operating as an 'empty shell';
f. ensure that they have appropriate governance and risk management arrangements in place to identify and manage their risks.

Competent authorities should take into account all risks in their assessment:

a. the operational risks posed by the outsourcing arrangement;
b. reputational risks;
c. the step-in risk that could require the institution to bail out a service provider, in the case of significant institutions;
d. concentration risks within the institution, including on a consolidated basis, caused by multiple outsourcing arrangements with a single service provider or closely connected service providers or multiple outsourcing arrangements within the same business area;
e. concentration risks at the sector level, e.g. where multiple institutions make use of a single service provider or a small group of service providers;
f. the extent to which the outsourcing institution controls the service provider or has the ability to influence its actions, the reduction of risks that may result from a higher level of control and if the service provider is included in the consolidated supervision of the group; and
g. conflicts of interest between the institution and the service provider.

Competent authorities should inform the resolution authority about new potentially critical functions that have been identified during this assessment. Where concerns are identified that lead to the conclusion that an institution no longer has robust governance arrangements in place or does not comply with regulatory requirements, competent authorities should take appropriate actions, which may include limiting or restricting the scope of the outsourced functions or requiring exit from one or more outsourcing arrangements.

In particular, taking into account the need of the institution to operate on a continuous basis, the cancellation of contracts could be required if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte Limited is the Cyprus member firm of DTTL. Deloitte Cyprus is among the nation's leading professional services firms, providing audit & assurance, consulting, financial advisory, wealth advisory, risk advisory, tax and related services as well as a complete range of services to international business through over 680 people in Nicosia and Limassol. For more information, please visit the Cyprus firm's website at www.deloitte.com/cy.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. Deloitte's approximately 286,000 professionals make an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019 Deloitte Limited